Council of the European Union

Brussels, 23 April 2021
(OR. en)

8115/21

**Interinstitutional File: 2021/0106(COD)**

**TELECOM 156**
**JAI 429**
**COPEN 191**
**CYBER 108**
**DATAPROTECT 103**
**EJUSTICE 41**
**COSI 69**
**IXIM 74**
**ENFOPOL 148**
**FREMP 103**
**RELEX 347**
**MI 271**
**COMPET 275**
**IA 60**
**CODEC 573**

**COVER NOTE**

| | |
|---|---|
| From: | Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director |
| date of receipt: | 22 April 2021 |
| To: | Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union |
| No. Cion doc.: | COM(2021) 206 final |
| Subject: | Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS |

Delegations will find attached document COM(2021) 206 final.

Encl.: COM(2021) 206 final

EUROPEAN
COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposal for a

# REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

# LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

# EXPLANATORY MEMORANDUM

## 1. CONTEXT OF THE PROPOSAL

### 1.1. Reasons for and objectives of the proposal

This explanatory memorandum accompanies the proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Artificial Intelligence (AI) is a fast evolving family of technologies that can bring a wide array of economic and societal benefits across the entire spectrum of industries and social activities. By improving prediction, optimising operations and resource allocation, and personalising service delivery, the use of artificial intelligence can support socially and environmentally beneficial outcomes and provide key competitive advantages to companies and the European economy. Such action is especially needed in high-impact sectors, including climate change, environment and health, the public sector, finance, mobility, home affairs and agriculture. However, the same elements and techniques that power the socio-economic benefits of AI can also bring about new risks or negative consequences for individuals or the society. In light of the speed of technological change and possible challenges, the EU is committed to strive for a balanced approach. It is in the Union interest to preserve the EU's technological leadership and to ensure that Europeans can benefit from new technologies developed and functioning according to Union values, fundamental rights and principles.

This proposal delivers on the political commitment by President von der Leyen, who announced in her political guidelines for the 2019-2024 Commission "A Union that strives for more"[1], that the Commission would put forward legislation for a coordinated European approach on the human and ethical implications of AI. Following on that announcement, on 19 February 2020 the Commission published the White Paper on AI - A European approach to excellence and trust[2]. The White Paper sets out policy options on how to achieve the twin objective of promoting the uptake of AI and of addressing the risks associated with certain uses of such technology. This proposal aims to implement the second objective for the development of an ecosystem of trust by proposing a legal framework for trustworthy AI. The proposal is based on EU values and fundamental rights and aims to give people and other users the confidence to embrace AI-based solutions, while encouraging businesses to develop them. AI should be a tool for people and be a force for good in society with the ultimate aim of increasing human well-being. Rules for AI available in the Union market or otherwise affecting people in the Union should therefore be human centric, so that people can trust that the technology is used in a way that is safe and compliant with the law, including the respect of fundamental rights. Following the publication of the White Paper, the Commission launched a broad stakeholder consultation, which was met with a great interest by a large number of stakeholders who were largely supportive of regulatory intervention to address the challenges and concerns raised by the increasing use of AI.

The proposal also responds to explicit requests from the European Parliament (EP) and the European Council, which have repeatedly expressed calls for legislative action to ensure a well-functioning internal market for artificial intelligence systems ('AI systems') where both

[1] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

[2] European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, 2020.

benefits and risks of AI are adequately addressed at Union level. It supports the objective of the Union being a global leader in the development of secure, trustworthy and ethical artificial intelligence as stated by the European Council[3] and ensures the protection of ethical principles as specifically requested by the European Parliament[4].

In 2017, the European Council called for a 'sense of urgency to address emerging trends' including 'issues such as artificial intelligence …, while at the same time ensuring a high level of data protection, digital rights and ethical standards'[5]. In its 2019 Conclusions on the Coordinated Plan on the development and use of artificial intelligence Made in Europe[6], the Council further highlighted the importance of ensuring that European citizens' rights are fully respected and called for a review of the existing relevant legislation to make it fit for purpose for the new opportunities and challenges raised by AI. The European Council has also called for a clear determination of the AI applications that should be considered high-risk[7].

The most recent Conclusions from 21 October 2020 further called for addressing the opacity, complexity, bias, a certain degree of unpredictability and partially autonomous behaviour of certain AI systems, to ensure their compatibility with fundamental rights and to facilitate the enforcement of legal rules[8].

The European Parliament has also undertaken a considerable amount of work in the area of AI. In October 2020, it adopted a number of resolutions related to AI, including on ethics[9], liability[10] and copyright[11]. In 2021, those were followed by resolutions on AI in criminal matters[12] and in education, culture and the audio-visual sector[13]. The EP Resolution on a Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies specifically recommends to the Commission to propose legislative action to harness the opportunities and benefits of AI, but also to ensure protection of ethical principles. The resolution includes a text of the legislative proposal for a regulation on ethical principles for

---

3 European Council, Special meeting of the European Council (1 and 2 October 2020) – Conclusions, EUCO 13/20, 2020, p. 6.

4 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

5 European Council, *European Council meeting (19 October 2017) – Conclusion* EUCO 14/17, 2017, p. 8.

6 Council of the European Union, *Artificial intelligence b) Conclusions on the coordinated plan on artificial intelligence-Adoption* 6177/19, 2019.

7 European Council, *Special meeting of the European Council (1and 2 October 2020) – Conclusions* EUCO 13/20, 2020.

8 Council of the European Union, *Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*, 11481/20, 2020.

9 European Parliament resolution of 20 October 2020 on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

10 European Parliament resolution of 20 October 2020 on a civil liability regime for artificial intelligence, 2020/2014(INL).

11 European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies, 2020/2015(INI).

12 European Parliament Draft Report, Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, 2020/2016(INI).

13 European Parliament Draft Report, Artificial intelligence in education, culture and the audiovisual sector, 2020/2017(INI). In that regard, the Commission has adopted the Digital Education Action Plan 2021-2027: Resetting education and training for the digital age, which foresees the development of ethical guidelines in AI and Data usage in education – Commission Communication COM(2020) 624 final.

the development, deployment and use of AI, robotics and related technologies. In accordance with the political commitment made by President von der Leyen in her Political Guidelines as regards resolutions adopted by the European Parliament under Article 225 TFEU, this proposal takes into account the aforementioned resolution of the European Parliament in full respect of proportionality, subsidiarity and better law making principles.

Against this political context, the Commission puts forward the proposed regulatory framework on Artificial Intelligence with the following **specific objectives**:

- ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;
- ensure legal certainty to facilitate investment and innovation in AI;
- enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
- facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

To achieve those objectives, this proposal presents a balanced and proportionate horizontal regulatory approach to AI that is limited to the minimum necessary requirements to address the risks and problems linked to AI, without unduly constraining or hindering technological development or otherwise disproportionately increasing the cost of placing AI solutions on the market. The proposal sets a robust and flexible legal framework. On the one hand, it is comprehensive and future-proof in its fundamental regulatory choices, including the principle-based requirements that AI systems should comply with. On the other hand, it puts in place a proportionate regulatory system centred on a well-defined risk-based regulatory approach that does not create unnecessary restrictions to trade, whereby legal intervention is tailored to those concrete situations where there is a justified cause for concern or where such concern can reasonably be anticipated in the near future. At the same time, the legal framework includes flexible mechanisms that enable it to be dynamically adapted as the technology evolves and new concerning situations emerge.

The proposal sets harmonised rules for the development, placement on the market and use of AI systems in the Union following a proportionate risk-based approach. It proposes a single future-proof definition of AI. Certain particularly harmful AI practices are prohibited as contravening Union values, while specific restrictions and safeguards are proposed in relation to certain uses of remote biometric identification systems for the purpose of law enforcement. The proposal lays down a solid risk methodology to define "high-risk" AI systems that pose significant risks to the health and safety or fundamental rights of persons. Those AI systems will have to comply with a set of horizontal mandatory requirements for trustworthy AI and follow conformity assessment procedures before those systems can be placed on the Union market. Predictable, proportionate and clear obligations are also placed on providers and users of those systems to ensure safety and respect of existing legislation protecting fundamental rights throughout the whole AI systems' lifecycle. For some specific AI systems, only minimum transparency obligations are proposed, in particular when chatbots or 'deep fakes' are used.

The proposed rules will be enforced through a governance system at Member States level, building on already existing structures, and a cooperation mechanism at Union level with the

establishment of a European Artificial Intelligence Board. Additional measures are also proposed to support innovation, in particular through AI regulatory sandboxes and other measures to reduce the regulatory burden and to support Small and Medium-Sized Enterprises ('SMEs') and start-ups.

### 1.2. Consistency with existing policy provisions in the policy area

The horizontal nature of the proposal requires full consistency with existing Union legislation applicable to sectors where high-risk AI systems are already used or likely to be used in the near future.

Consistency is also ensured with the EU Charter of Fundamental Rights and the existing secondary Union legislation on data protection, consumer protection, non-discrimination and gender equality. The proposal is without prejudice and complements the General Data Protection Regulation (Regulation (EU) 2016/679) and the Law Enforcement Directive (Directive (EU) 2016/680) with a set of harmonised rules applicable to the design, development and use of certain high-risk AI systems and restrictions on certain uses of remote biometric identification systems. Furthermore, the proposal complements existing Union law on non-discrimination with specific requirements that aim to minimise the risk of algorithmic discrimination, in particular in relation to the design and the quality of data sets used for the development of AI systems complemented with obligations for testing, risk management, documentation and human oversight throughout the AI systems' lifecycle. The proposal is without prejudice to the application of Union competition law.

As regards high-risk AI systems which are safety components of products, this proposal will be integrated into the existing sectoral safety legislation to ensure consistency, avoid duplications and minimise additional burdens. In particular, as regards high-risk AI systems related to products covered by the New Legislative Framework (NLF) legislation (e.g. machinery, medical devices, toys), the requirements for AI systems set out in this proposal will be checked as part of the existing conformity assessment procedures under the relevant NLF legislation. With regard to the interplay of requirements, while the safety risks specific to AI systems are meant to be covered by the requirements of this proposal, NLF legislation aims at ensuring the overall safety of the final product and therefore may contain specific requirements regarding the safe integration of an AI system into the final product. The proposal for a Machinery Regulation, which is adopted on the same day as this proposal fully reflects this approach. As regards high-risk AI systems related to products covered by relevant Old Approach legislation (e.g. aviation, cars), this proposal would not directly apply. However, the ex-ante essential requirements for high-risk AI systems set out in this proposal will have to be taken into account when adopting relevant implementing or delegated legislation under those acts.

As regards AI systems provided or used by regulated credit institutions, the authorities responsible for the supervision of the Union's financial services legislation should be designated as competent authorities for supervising the requirements in this proposal to ensure a coherent enforcement of the obligations under this proposal and the Union's financial services legislation where AI systems are to some extent implicitly regulated in relation to the internal governance system of credit institutions. To further enhance consistency, the conformity assessment procedure and some of the providers' procedural obligations under this

proposal are integrated into the procedures under Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision[14].

This proposal is also consistent with the applicable Union legislation on services, including on intermediary services regulated by the e-Commerce Directive 2000/31/EC[15] and the Commission's recent proposal for the Digital Services Act (DSA)[16].

In relation to AI systems that are components of large-scale IT systems in the Area of Freedom, Security and Justice managed by the European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA), the proposal will not apply to those AI systems that have been placed on the market or put into service before one year has elapsed from the date of application of this Regulation, unless the replacement or amendment of those legal acts leads to a significant change in the design or intended purpose of the AI system or AI systems concerned.

### 1.3. Consistency with other Union policies

The proposal is part of a wider comprehensive package of measures that address problems posed by the development and use of AI, as examined in the White Paper on AI. Consistency and complementarity is therefore ensured with other ongoing or planned initiatives of the Commission that also aim to address those problems, including the revision of sectoral product legislation (e.g. the Machinery Directive, the General Product Safety Directive) and initiatives that address liability issues related to new technologies, including AI systems. Those initiatives will build on and complement this proposal in order to bring legal clarity and foster the development of an ecosystem of trust in AI in Europe.

The proposal is also coherent with the Commission's overall digital strategy in its contribution to promoting technology that works for people, one of the three main pillars of the policy orientation and objectives announced in the Communication 'Shaping Europe's digital future'[17]. It lays down a coherent, effective and proportionate framework to ensure AI is developed in ways that respect people's rights and earn their trust, making Europe fit for the digital age and turning the next ten years into the **Digital Decade**[18].

Furthermore, the promotion of AI-driven innovation is closely linked to the **Data Governance Act**[19]**,** the **Open Data Directive**[20] and other initiatives under **the EU strategy for data**[21], which will establish trusted mechanisms and services for the re-use, sharing and

---

14 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC Text with EEA relevance, OJ L 176, 27.6.2013, p. 338–436.

15 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16.

16 See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final.

17 Communication from the Commission, Shaping Europe's Digital Future, COM/2020/67 final.

18 2030 Digital Compass: the European way for the Digital Decade.

19 Proposal for a Regulation on European data governance (Data Governance Act) COM/2020/767.

20 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83.

21 Commission Communication, A European strategy for data COM/2020/66 final.

pooling of data that are essential for the development of data-driven AI models of high quality.

The proposal also strengthens significantly the Union's role to help shape global norms and standards and promote trustworthy AI that is consistent with Union values and interests. It provides the Union with a powerful basis to engage further with its external partners, including third countries, and at international fora on issues relating to AI.

## 2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

### 2.1. Legal basis

The legal basis for the proposal is in the first place Article 114 of the Treaty on the Functioning of the European Union (TFEU), which provides for the adoption of measures to ensure the establishment and functioning of the internal market.

This proposal constitutes a core part of the EU digital single market strategy. The primary objective of this proposal is to ensure the proper functioning of the internal market by setting harmonised rules in particular on the development, placing on the Union market and the use of products and services making use of AI technologies or provided as stand-alone AI systems. Some Member States are already considering national rules to ensure that AI is safe and is developed and used in compliance with fundamental rights obligations. This will likely lead to two main problems: i) a fragmentation of the internal market on essential elements regarding in particular the requirements for the AI products and services, their marketing, their use, the liability and the supervision by public authorities, and ii) the substantial diminishment of legal certainty for both providers and users of AI systems on how existing and new rules will apply to those systems in the Union. Given the wide circulation of products and services across borders, these two problems can be best solved through EU harmonizing legislation.

Indeed, the proposal defines common mandatory requirements applicable to the design and development of certain AI systems before they are placed on the market that will be further operationalised through harmonised technical standards. The proposal also addresses the situation after AI systems have been placed on the market by harmonising the way in which ex-post controls are conducted.

In addition, considering that this proposal contains certain specific rules on the protection of individuals with regard to the processing of personal data, notably restrictions of the use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces for the purpose of law enforcement, it is appropriate to base this regulation, in as far as those specific rules are concerned, on Article 16 of the TFEU.

### 2.2. Subsidiarity (for non-exclusive competence)

The nature of AI, which often relies on large and varied datasets and which may be embedded in any product or service circulating freely within the internal market, entails that the objectives of this proposal cannot be effectively achieved by Member States alone. Furthermore, an emerging patchwork of potentially divergent national rules will hamper the

seamless circulation of products and services related to AI systems across the EU and will be ineffective in ensuring the safety and protection of fundamental rights and Union values across the different Member States. National approaches in addressing the problems will only create additional legal uncertainty and barriers, and will slow market uptake of AI.

The objectives of this proposal can be better achieved at Union level to avoid a further fragmentation of the Single Market into potentially contradictory national frameworks preventing the free circulation of goods and services embedding AI. A solid European regulatory framework for trustworthy AI will also ensure a level playing field and protect all people, while strengthening Europe's competitiveness and industrial basis in AI. Only common action at Union level can also protect the Union's digital sovereignty and leverage its tools and regulatory powers to shape global rules and standards.

### 2.3. Proportionality

The proposal builds on existing legal frameworks and is proportionate and necessary to achieve its objectives, since it follows a risk-based approach and imposes regulatory burdens only when an AI system is likely to pose high risks to fundamental rights and safety. For other, non-high-risk AI systems, only very limited transparency obligations are imposed, for example in terms of the provision of information to flag the use of an AI system when interacting with humans. For high-risk AI systems, the requirements of high quality data, documentation and traceability, transparency, human oversight, accuracy and robustness, are strictly necessary to mitigate the risks to fundamental rights and safety posed by AI and that are not covered by other existing legal frameworks. Harmonised standards and supporting guidance and compliance tools will assist providers and users in complying with the requirements laid down by the proposal and minimise their costs. The costs incurred by operators are proportionate to the objectives achieved and the economic and reputational benefits that operators can expect from this proposal.

### 2.4. Choice of the instrument

The choice of a regulation as a legal instrument is justified by the need for a uniform application of the new rules, such as definition of AI, the prohibition of certain harmful AI-enabled practices and the classification of certain AI systems. The direct applicability of a Regulation, in accordance with Article 288 TFEU, will reduce legal fragmentation and facilitate the development of a single market for lawful, safe and trustworthy AI systems. It will do so, in particular, by introducing a harmonised set of core requirements with regard to AI systems classified as high-risk and obligations for providers and users of those systems, improving the protection of fundamental rights and providing legal certainty for operators and consumers alike.

At the same time, the provisions of the regulation are not overly prescriptive and leave room for different levels of Member State action for elements that do not undermine the objectives of the initiative, in particular the internal organisation of the market surveillance system and the uptake of measures to foster innovation.

## 3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

### 3.1. Stakeholder consultation

This proposal is the result of extensive consultation with all major stakeholders, in which the general principles and minimum standards for consultation of interested parties by the Commission were applied.

An **online public consultation** was launched on 19 February 2020 along with the publication of the White Paper on Artificial Intelligence and ran until 14 June 2020. The objective of that consultation was to collect views and opinions on the White Paper. It targeted all interested stakeholders from the public and private sectors, including governments, local authorities, commercial and non-commercial organisations, social partners, experts, academics and citizens. After analysing all the responses received, the Commission published a summary outcome and the individual responses on its website[22].

In total, 1215 contributions were received, of which 352 were from companies or business organisations/associations, 406 from individuals (92%individuals from EU ), 152 on behalf of academic/research institutions, and 73 from public authorities. Civil society's voices were represented by 160 respondents (among which 9 consumers' organisations, 129 non-governmental organisations and 22 trade unions), 72 respondents contributed as 'others'. Of the 352 business and industry representatives, 222 were companies and business representatives, 41.5% of which were micro, small and medium-sized enterprises. The rest were business associations. Overall, 84% of business and industry replies came from the EU-27. Depending on the question, between 81 and 598 of the respondents used the free text option to insert comments. Over 450 position papers were submitted through the EU Survey website, either in addition to questionnaire answers (over 400) or as stand-alone contributions (over 50).

Overall, there is a general agreement amongst stakeholders on a need for action. A large majority of stakeholders agree that legislative gaps exist or that new legislation is needed. However, several stakeholders warn the Commission to avoid duplication, conflicting obligations and overregulation. There were many comments underlining the importance of a technology neutral and proportionate regulatory framework.

Stakeholders mostly requested a narrow, clear and precise definition for AI. Stakeholders also highlighted that besides the clarification of the term of AI, it is important to define 'risk', 'high-risk', 'low-risk', 'remote biometric identification' and 'harm'.

Most of the respondents are explicitly in favour of the risk-based approach. Using a risk-based framework was considered a better option than blanket regulation of all AI systems. The types of risks and threats should be based on a sector-by-sector and case-by-case approach. Risks also should be calculated taking into account the impact on rights and safety.

Regulatory sandboxes could be very useful for the promotion of AI and are welcomed by certain stakeholders, especially the Business Associations.

---

22 See all consultation results here.

Among those who formulated their opinion on the enforcement models, more than 50%, especially from the business associations, were in favour of a combination of an ex-ante risk self-assessment and an ex-post enforcement for high-risk AI systems.

### 3.2. Collection and use of expertise

The proposal builds on two years of analysis and close involvement of stakeholders, including academics, businesses, social partners, non-governmental organisations, Member States and citizens. The preparatory work started in 2018 with the setting up of a **High-Level Expert Group on AI (HLEG)** which had an inclusive and broad composition of 52 well-known experts tasked to advise the Commission on the implementation of the Commission's Strategy on Artificial Intelligence. In April 2019, the Commission supported[23] the key requirements set out in the HLEG ethics guidelines for Trustworthy AI[24], which had been revised to take into account more than 500 submissions from stakeholders. The key requirements reflect a widespread and common approach, as evidenced by a plethora of ethical codes and principles developed by many private and public organisations in Europe and beyond, that AI development and use should be guided by certain essential value-oriented principles. The Assessment List for Trustworthy Artificial Intelligence (ALTAI)[25] made those requirements operational in a piloting process with over 350 organisations.

In addition, the **AI Alliance**[26] was formed as a platform for approximately 4000 stakeholders to debate the technological and societal implications of AI, culminating in a yearly AI Assembly.

The **White Paper** on AI further developed this inclusive approach, inciting comments from more than 1250 stakeholders, including over 450 additional position papers. As a result, the Commission published an Inception Impact Assessment, which in turn attracted more than 130 comments[27]. **Additional stakeholder workshops and events** were also organised the results of which support the analysis in the impact assessment and the policy choices made in this proposal[28]. An **external study** was also procured to feed into the impact assessment.

### 3.3. Impact assessment

In line with its "Better Regulation" policy, the Commission conducted an impact assessment for this proposal examined by the Commission's Regulatory Scrutiny Board. A meeting with the Regulatory Scrutiny Board was held on 16 December 2020, which was followed by a negative opinion. After substantial revision of the impact assessment to address the comments and a resubmission of the impact assessment, the Regulatory Scrutiny Board issued a positive opinion on 21 March 2021. The opinions of the Regulatory Scrutiny Board, the recommendations and an explanation of how they have been taken into account are presented in Annex 1 of the impact assessment.

---

23 European Commission, *Building Trust in Human-Centric Artificial Intelligence*, COM(2019) 168.

24 HLEG, *Ethics Guidelines for Trustworthy AI*, 2019.

25 HLEG, *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*, 2020.

26 The AI Alliance is a multi-stakeholder forum launched in June 2018, AI Alliance https://ec.europa.eu/digital-single-market/en/european-ai-alliance

27 European Commission, *Inception Impact Assessment For a Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence.*

28 For details of all the consultations that have been carried out see Annex 2 of the impact assessment.

The Commission examined different policy options to achieve the general objective of the proposal, which is to **ensure the proper functioning of the single market** by creating the conditions for the development and use of trustworthy AI in the Union.

Four policy options of different degrees of regulatory intervention were assessed:

- **Option 1**: EU legislative instrument setting up a voluntary labelling scheme;
- **Option 2**: a sectoral, "ad-hoc" approach;
- **Option 3**: Horizontal EU legislative instrument following a proportionate risk-based approach;
- **Option 3+**: Horizontal EU legislative instrument following a proportionate risk-based approach + codes of conduct for non-high-risk AI systems;
- **Option 4**: Horizontal EU legislative instrument establishing mandatory requirements for all AI systems, irrespective of the risk they pose.

According to the Commission's established methodology, each policy option was evaluated against economic and societal impacts, with a particular focus on impacts on fundamental rights. The preferred option is option 3+, a regulatory framework for high-risk AI systems only, with the possibility for all providers of non-high-risk AI systems to follow a code of conduct. The requirements will concern data, documentation and traceability, provision of information and transparency, human oversight and robustness and accuracy and would be mandatory for high-risk AI systems. Companies that introduced codes of conduct for other AI systems would do so voluntarily.

The preferred option was considered suitable to address in the most effective way the objectives of this proposal. By requiring a restricted yet effective set of actions from AI developers and users, the preferred option limits the risks of violation of fundamental rights and safety of people and foster effective supervision and enforcement, by targeting the requirements only to systems where there is a high risk that such violations could occur. As a result, that option keeps compliance costs to a minimum, thus avoiding an unnecessary slowing of uptake due to higher prices and compliance costs. In order to address possible disadvantages for SMEs, this option includes several provisions to support their compliance and reduce their costs, including creation of regulatory sandboxes and obligation to consider SMEs interests when setting fees related to conformity assessment.

The preferred option will increase people's trust in AI, companies will gain in legal certainty, and Member States will see no reason to take unilateral action that could fragment the single market. As a result of higher demand due to higher trust, more available offers due to legal certainty, and the absence of obstacles to cross-border movement of AI systems, the single market for AI will likely flourish. The European Union will continue to develop a fast-growing AI ecosystem of innovative services and products embedding AI technology or stand-alone AI systems, resulting in increased digital autonomy.

Businesses or public authorities that develop or use AI applications that constitute a high risk for the safety or fundamental rights of citizens would have to comply with specific requirements and obligations. Compliance with these requirements would imply costs amounting to approximately EUR € 6000 to EUR € 7000 for the supply of an average high-risk AI system of around EUR € 170000 by 2025. For AI users, there would also be the

annual cost for the time spent on ensuring human oversight where this is appropriate, depending on the use case. Those have been estimated at approximately EUR € 5000 to EUR € 8000 per year. Verification costs could amount to another EUR € 3000 to EUR € 7500 for suppliers of high-risk AI. Businesses or public authorities that develop or use any AI applications not classified as high risk would only have minimal obligations of information. However, they could choose to join others and together adopt a code of conduct to follow suitable requirements, and to ensure that their AI systems are trustworthy. In such a case, costs would be at most as high as for high-risk AI systems, but most probably lower.

The impacts of the policy options on different categories of stakeholders (economic operators/ business; conformity assessment bodies, standardisation bodies and other public bodies; individuals/citizens; researchers) are explained in detail in Annex 3 of the Impact assessment supporting this proposal.

### 3.4. Regulatory fitness and simplification

This proposal lays down obligation that will apply to providers and users of high-risk AI systems. For providers who develop and place such systems on the Union market, it will create legal certainty and ensure that no obstacle to the cross-border provision of AI-related services and products emerge. For companies using AI, it will promote trust among their customers. For national public administrations, it will promote public trust in the use of AI and strengthen enforcement mechanisms (by introducing a European coordination mechanism, providing for appropriate capacities, and facilitating audits of the AI systems with new requirements for documentation, traceability and transparency). Moreover, the framework will envisage specific measures supporting innovation, including regulatory sandboxes and specific measures supporting small-scale users and providers of high-risk AI systems to comply with the new rules.

The proposal also specifically aims at strengthening Europe's competitiveness and industrial basis in AI. Full consistency is ensured with existing sectoral Union legislation applicable to AI systems (e.g. on products and services) that will bring further clarity and simplify the enforcement of the new rules.

### 3.5. Fundamental rights

The use of AI with its specific characteristics (e.g. opacity, complexity, dependency on data, autonomous behaviour) can adversely affect a number of fundamental rights enshrined in the EU Charter of Fundamental Rights ('the Charter'). This proposal seeks to ensure a high level of protection for those fundamental rights and aims to address various sources of risks through a clearly defined risk-based approach. With a set of requirements for trustworthy AI and proportionate obligations on all value chain participants, the proposal will enhance and promote the protection of the rights protected by the Charter: the right to human dignity (Article 1), respect for private life and protection of personal data (Articles 7 and 8), non-discrimination (Article 21) and equality between women and men (Article 23). It aims to prevent a chilling effect on the rights to freedom of expression (Article 11) and freedom of assembly (Article 12), to ensure protection of the right to an effective remedy and to a fair trial, the rights of defence and the presumption of innocence (Articles 47 and 48), as well as the general principle of good administration. Furthermore, as applicable in certain domains, the proposal will positively affect the rights of a number of special groups, such as the workers' rights to fair and just working conditions (Article 31), a high level of consumer protection (Article 28), the rights of the child (Article 24) and the integration of persons with

disabilities (Article 26). The right to a high level of environmental protection and the improvement of the quality of the environment (Article 37) is also relevant, including in relation to the health and safety of people. The obligations for ex ante testing, risk management and human oversight will also facilitate the respect of other fundamental rights by minimising the risk of erroneous or biased AI-assisted decisions in critical areas such as education and training, employment, important services, law enforcement and the judiciary. In case infringements of fundamental rights still happen, effective redress for affected persons will be made possible by ensuring transparency and traceability of the AI systems coupled with strong ex post controls.

This proposal imposes some restrictions on the freedom to conduct business (Article 16) and the freedom of art and science (Article 13) to ensure compliance with overriding reasons of public interest such as health, safety, consumer protection and the protection of other fundamental rights ('responsible innovation') when high-risk AI technology is developed and used. Those restrictions are proportionate and limited to the minimum necessary to prevent and mitigate serious safety risks and likely infringements of fundamental rights.

The increased transparency obligations will also not disproportionately affect the right to protection of intellectual property (Article 17(2)), since they will be limited only to the minimum necessary information for individuals to exercise their right to an effective remedy and to the necessary transparency towards supervision and enforcement authorities, in line with their mandates. Any disclosure of information will be carried out in compliance with relevant legislation in the field, including Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. When public authorities and notified bodies need to be given access to confidential information or source code to examine compliance with substantial obligations, they are placed under binding confidentiality obligations.

## 4. BUDGETARY IMPLICATIONS

Member States will have to designate supervisory authorities in charge of implementing the legislative requirements. Their supervisory function could build on existing arrangements, for example regarding conformity assessment bodies or market surveillance, but would require sufficient technological expertise and human and financial resources. Depending on the pre-existing structure in each Member State, this could amount to 1 to 25 Full Time Equivalents per Member State.

A detailed overview of the costs involved is provided in the 'financial statement' linked to this proposal.

## 5. OTHER ELEMENTS

### 5.1. Implementation plans and monitoring, evaluation and reporting arrangements

Providing for a robust monitoring and evaluation mechanism is crucial to ensure that the proposal will be effective in achieving its specific objectives. The Commission will be in charge of monitoring the effects of the proposal. It will establish a system for registering stand-alone high-risk AI applications in a public EU-wide database. This registration will also enable competent authorities, users and other interested people to verify if the high-risk AI system complies with the requirements laid down in the proposal and to exercise enhanced

oversight over those AI systems posing high risks to fundamental rights. To feed this database, AI providers will be obliged to provide meaningful information about their systems and the conformity assessment carried out on those systems.

Moreover, AI providers will be obliged to inform national competent authorities about serious incidents or malfunctioning that constitute a breach of fundamental rights obligations as soon as they become aware of them, as well as any recalls or withdrawals of AI systems from the market. National competent authorities will then investigate the incidents/or malfunctioning, collect all the necessary information and regularly transmit it to the Commission with adequate metadata. The Commission will complement this information on the incidents by a comprehensive analysis of the overall market for AI.

The Commission will publish a report evaluating and reviewing the proposed AI framework five years following the date on which it becomes applicable.

## 5.2. Detailed explanation of the specific provisions of the proposal

### *5.2.1. SCOPE AND DEFINITIONS (TITLE I)*

**Title I** defines the subject matter of the regulation and the scope of application of the new rules that cover the placing on the market, putting into service and use of AI systems. It also sets out the definitions used throughout the instrument. The definition of AI system in the legal framework aims to be as technology neutral and future proof as possible, taking into account the fast technological and market developments related to AI. In order to provide the needed legal certainty, Title I is complemented by Annex I, which contains a detailed list of approaches and techniques for the development of AI to be adapted by the Commission in line with new technological developments. Key participants across the AI value chain are also clearly defined such as providers and users of AI systems that cover both public and private operators to ensure a level playing field.

### *5.2.2. PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES (TITLE II)*

**Title II** establishes a list of prohibited AI. The regulation follows a risk-based approach, differentiating between uses of AI that create (i) an unacceptable risk, (ii) a high risk, and (iii) low or minimal risk. The list of prohibited practices in Title II comprises all those AI systems whose use is considered unacceptable as contravening Union values, for instance by violating fundamental rights. The prohibitions covers practices that have a significant potential to manipulate persons through subliminal techniques beyond their consciousness or exploit vulnerabilities of specific vulnerable groups such as children or persons with disabilities in order to materially distort their behaviour in a manner that is likely to cause them or another person psychological or physical harm. Other manipulative or exploitative practices affecting adults that might be facilitated by AI systems could be covered by the existing data protection, consumer protection and digital service legislation that guarantee that natural persons are properly informed and have free choice not to be subject to profiling or other practices that might affect their behaviour. The proposal also prohibits AI-based social scoring for general purposes done by public authorities. Finally, the use of 'real time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement is also prohibited unless certain limited exceptions apply.

### *5.2.3. HIGH-RISK AI SYSTEMS (TITLE III)*

**Title III** contains specific rules for AI systems that create a high risk to the health and safety or fundamental rights of natural persons. In line with a risk-based approach, those high-risk AI systems are permitted on the European market subject to compliance with certain mandatory requirements and an ex-ante conformity assessment. The classification of an AI system as high-risk is based on the intended purpose of the AI system, in line with existing product safety legislation. Therefore, the classification as high-risk does not only depend on the function performed by the AI system, but also on the specific purpose and modalities for which that system is used.

Chapter 1 of Title III sets the classification rules and identifies two main categories of high-risk AI systems:

- AI systems intended to be used as safety component of products that are subject to third party ex-ante conformity assessment;
- other stand-alone AI systems with mainly fundamental rights implications that are explicitly listed in Annex III.

This list of high-risk AI systems in Annex III contains a limited number of AI systems whose risks have already materialised or are likely to materialise in the near future. To ensure that the regulation can be adjusted to emerging uses and applications of AI, the Commission may expand the list of high-risk AI systems used within certain pre-defined areas, by applying a set of criteria and risk assessment methodology.

Chapter 2 sets out the legal requirements for high-risk AI systems in relation to data and data governance, documentation and recording keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security. The proposed minimum requirements are already state-of-the-art for many diligent operators and the result of two years of preparatory work, derived from the Ethics Guidelines of the HLEG[29], piloted by more than 350 organisations[30]. They are also largely consistent with other international recommendations and principles, which ensures that the proposed AI framework is compatible with those adopted by the EU's international trade partners. The precise technical solutions to achieve compliance with those requirements may be provided by standards or by other technical specifications or otherwise be developed in accordance with general engineering or scientific knowledge at the discretion of the provider of the AI system. This flexibility is particularly important, because it allows providers of AI systems to choose the way to meet their requirements, taking into account the state-of-the-art and technological and scientific progress in this field.

Chapter 3 places a clear set of horizontal obligations on providers of high-risk AI systems. Proportionate obligations are also placed on users and other participants across the AI value chain (e.g., importers, distributors, authorized representatives).

Chapter 4 sets the framework for notified bodies to be involved as independent third parties in conformity assessment procedures, while Chapter 5 explains in detail the conformity

[29] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 2019.

[30] They were also endorsed by the Commission in its 2019 Communication on human-centric approach to AI.

assessment procedures to be followed for each type of high-risk AI system. The conformity assessment approach aims to minimise the burden for economic operators as well as for notified bodies, whose capacity needs to be progressively ramped up over time. AI systems intended to be used as safety components of products that are regulated under the New Legislative Framework legislation (e.g. machinery, toys, medical devices, etc.) will be subject to the same ex-ante and ex-post compliance and enforcement mechanisms of the products of which they are a component. The key difference is that the ex-ante and ex-post mechanisms will ensure compliance not only with the requirements established by sectorial legislation, but also with the requirements established by this regulation.

As regards stand-alone high-risk AI systems that are referred to in Annex III, a new compliance and enforcement system will be established. This follows the model of the New Legislative Framework legislation implemented through internal control checks by the providers with the exception of remote biometric identification systems that would be subject to third party conformity assessment. A comprehensive ex-ante conformity assessment through internal checks, combined with a strong ex-post enforcement, could be an effective and reasonable solution for those systems, given the early phase of the regulatory intervention and the fact the AI sector is very innovative and expertise for auditing is only now being accumulated. An assessment through internal checks for 'stand-alone' high-risk AI systems would require a full, effective and properly documented ex ante compliance with all requirements of the regulation and compliance with robust quality and risk management systems and post-market monitoring. After the provider has performed the relevant conformity assessment, it should register those stand-alone high-risk AI systems in an EU database that will be managed by the Commission to increase public transparency and oversight and strengthen ex post supervision by competent authorities. By contrast, for reasons of consistency with the existing product safety legislation, the conformity assessments of AI systems that are safety components of products will follow a system with third party conformity assessment procedures already established under the relevant sectoral product safety legislation. New ex ante re-assessments of the conformity will be needed in case of substantial modifications to the AI systems (and notably changes which go beyond what is pre-determined by the provider in its technical documentation and checked at the moment of the ex-ante conformity assessment).

### *5.2.4. TRANSPARENCY OBLIGATIONS FOR CERTAIN AI SYSTEMS (TITLE IV)*

**Title IV** concerns certain AI systems to take account of the specific risks of manipulation they pose. Transparency obligations will apply for systems that (i) interact with humans, (ii) are used to detect emotions or determine association with (social) categories based on biometric data, or (iii) generate or manipulate content ('deep fakes'). When persons interact with an AI system or their emotions or characteristics are recognised through automated means, people must be informed of that circumstance. If an AI system is used to generate or manipulate image, audio or video content that appreciably resembles authentic content, there should be an obligation to disclose that the content is generated through automated means, subject to exceptions for legitimate purposes (law enforcement, freedom of expression). This allows persons to make informed choices or step back from a given situation.

### *5.2.5. MEASURES IN SUPPORT OF INNOVATION (TITLE V)*

**Title V** contributes to the objective to create a legal framework that is innovation-friendly, future-proof and resilient to disruption. To that end, it encourages national competent authorities to set up regulatory sandboxes and sets a basic framework in terms of governance,

supervision and liability. AI regulatory sandboxes establish a controlled environment to test innovative technologies for a limited time on the basis of a testing plan agreed with the competent authorities. Title V also contains measures to reduce the regulatory burden on SMEs and start-ups.

*5.2.6. GOVERNANCE AND IMPLEMENTATION (TITLES VI, VII AND VII)*

**Title VI** sets up the governance systems at Union and national level. At Union level, the proposal establishes a European Artificial Intelligence Board (the 'Board'), composed of representatives from the Member States and the Commission. The Board will facilitate a smooth, effective and harmonised implementation of this regulation by contributing to the effective cooperation of the national supervisory authorities and the Commission and providing advice and expertise to the Commission. It will also collect and share best practices among the Member States.

At national level, Member States will have to designate one or more national competent authorities and, among them, the national supervisory authority, for the purpose of supervising the application and implementation of the regulation. The European Data Protection Supervisor will act as the competent authority for the supervision of the Union institutions, agencies and bodies when they fall within the scope of this regulation.

**Title VII** aims to facilitate the monitoring work of the Commission and national authorities through the establishment of an EU-wide database for stand-alone high-risk AI systems with mainly fundamental rights implications. The database will be operated by the Commission and provided with data by the providers of the AI systems, who will be required to register their systems before placing them on the market or otherwise putting them into service.

**Title VIII** sets out the monitoring and reporting obligations for providers of AI systems with regard to post-market monitoring and reporting and investigating on AI-related incidents and malfunctioning. Market surveillance authorities would also control the market and investigate compliance with the obligations and requirements for all high-risk AI systems already placed on the market. Market surveillance authorities would have all powers under Regulation (EU) 2019/1020 on market surveillance. Ex-post enforcement should ensure that once the AI system has been put on the market, public authorities have the powers and resources to intervene in case AI systems generate unexpected risks, which warrant rapid action. They will also monitor compliance of operators with their relevant obligations under the regulation. The proposal does not foresee the automatic creation of any additional bodies or authorities at Member State level. Member States may therefore appoint (and draw upon the expertise of) existing sectorial authorities, who would be entrusted also with the powers to monitor and enforce the provisions of the regulation.

All this is without prejudice to the existing system and allocation of powers of ex-post enforcement of obligations regarding fundamental rights in the Member States. When necessary for their mandate, existing supervision and enforcement authorities will also have the power to request and access any documentation maintained following this regulation and, where needed, request market surveillance authorities to organise testing of the high-risk AI system through technical means.

*5.2.7. CODES OF CONDUCT (TITLE IX)*

**Title IX** creates a framework for the creation of codes of conduct, which aim to encourage providers of non-high-risk AI systems to apply voluntarily the mandatory requirements for

high-risk AI systems (as laid out in Title III). Providers of non-high-risk AI systems may create and implement the codes of conduct themselves. Those codes may also include voluntary commitments related, for example, to environmental sustainability, accessibility for persons with disability, stakeholders' participation in the design and development of AI systems, and diversity of development teams.

*5.2.8. FINAL PROVISIONS (TITLES X, XI AND XII)*

**Title X** emphasizes the obligation of all parties to respect the confidentiality of information and data and sets out rules for the exchange of information obtained during the implementation of the regulation. Title X also includes measures to ensure the effective implementation of the regulation through effective, proportionate, and dissuasive penalties for infringements of the provisions.

**Title XI** sets out rules for the exercise of delegation and implementing powers. The proposal empowers the Commission to adopt, where appropriate, implementing acts to ensure uniform application of the regulation or delegated acts to update or complement the lists in Annexes I to VII.

**Title XII** contains an obligation for the Commission to assess regularly the need for an update of Annex III and to prepare regular reports on the evaluation and review of the regulation. It also lays down final provisions, including a differentiated transitional period for the initial date of the applicability of the regulation to facilitate the smooth implementation for all parties concerned.

2021/0106 (COD)

Proposal for a

# REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

# LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[31],

Having regard to the opinion of the Committee of the Regions[32],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, marketing and use of artificial intelligence in conformity with Union values. This Regulation pursues a number of overriding reasons of public interest, such as a high level of protection of health, safety and fundamental rights, and it ensures the free movement of AI-based goods and services cross-border, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation.

(2) Artificial intelligence systems (AI systems) can be easily deployed in multiple sectors of the economy and society, including cross border, and circulate throughout the Union. Certain Member States have already explored the adoption of national rules to ensure that artificial intelligence is safe and is developed and used in compliance with fundamental rights obligations. Differing national rules may lead to fragmentation of the internal market and decrease legal certainty for operators that develop or use AI systems. A consistent and high level of protection throughout the Union should therefore be ensured, while divergences hampering the free circulation of AI systems and related products and services within the internal market should be prevented, by

[31] OJ C […], […], p. […].
[32] OJ C […], […], p. […].

laying down uniform obligations for operators and guaranteeing the uniform protection of overriding reasons of public interest and of rights of persons throughout the internal market based on Article 114 of the Treaty on the Functioning of the European Union (TFEU). To the extent that this Regulation contains specific rules on the protection of individuals with regard to the processing of personal data concerning restrictions of the use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces for the purpose of law enforcement, it is appropriate to base this Regulation, in as far as those specific rules are concerned, on Article 16 of the TFEU. In light of those specific rules and the recourse to Article 16 TFEU, it is appropriate to consult the European Data Protection Board.

(3) Artificial intelligence is a fast evolving family of technologies that can contribute to a wide array of economic and societal benefits across the entire spectrum of industries and social activities. By improving prediction, optimising operations and resource allocation, and personalising digital solutions available for individuals and organisations, the use of artificial intelligence can provide key competitive advantages to companies and support socially and environmentally beneficial outcomes, for example in healthcare, farming, education and training, infrastructure management, energy, transport and logistics, public services, security, justice, resource and energy efficiency, and climate change mitigation and adaptation.

(4) At the same time, depending on the circumstances regarding its specific application and use, artificial intelligence may generate risks and cause harm to public interests and rights that are protected by Union law. Such harm might be material or immaterial.

(5) A Union legal framework laying down harmonised rules on artificial intelligence is therefore needed to foster the development, use and uptake of artificial intelligence in the internal market that at the same time meets a high level of protection of public interests, such as health and safety and the protection of fundamental rights, as recognised and protected by Union law. To achieve that objective, rules regulating the placing on the market and putting into service of certain AI systems should be laid down, thus ensuring the smooth functioning of the internal market and allowing those systems to benefit from the principle of free movement of goods and services. By laying down those rules, this Regulation supports the objective of the Union of being a global leader in the development of secure, trustworthy and ethical artificial intelligence, as stated by the European Council[33], and it ensures the protection of ethical principles, as specifically requested by the European Parliament[34].

(6) The notion of AI system should be clearly defined to ensure legal certainty, while providing the flexibility to accommodate future technological developments. The definition should be based on the key functional characteristics of the software, in particular the ability, for a given set of human-defined objectives, to generate outputs such as content, predictions, recommendations, or decisions which influence the environment with which the system interacts, be it in a physical or digital dimension.

---

33 European Council, Special meeting of the European Council (1 and 2 October 2020) – Conclusions, EUCO 13/20, 2020, p. 6.

34 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

AI systems can be designed to operate with varying levels of autonomy and be used on a stand-alone basis or as a component of a product, irrespective of whether the system is physically integrated into the product (embedded) or serve the functionality of the product without being integrated therein (non-embedded). The definition of AI system should be complemented by a list of specific techniques and approaches used for its development, which should be kept up-to–date in the light of market and technological developments through the adoption of delegated acts by the Commission to amend that list.

(7) The notion of biometric data used in this Regulation is in line with and should be interpreted consistently with the notion of biometric data as defined in Article 4(14) of Regulation (EU) 2016/679 of the European Parliament and of the Council[35], Article 3(18) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[36] and Article 3(13) of Directive (EU) 2016/680 of the European Parliament and of the Council[37].

(8) The notion of remote biometric identification system as used in this Regulation should be defined functionally, as an AI system intended for the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used. Considering their different characteristics and manners in which they are used, as well as the different risks involved, a distinction should be made between 'real-time' and 'post' remote biometric identification systems. In the case of 'real-time' systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay. In this regard, there should be no scope for circumventing the rules of this Regulation on the 'real-time' use of the AI systems in question by providing for minor delays. 'Real-time' systems involve the use of 'live' or 'near-'live' material, such as video footage, generated by a camera or other device with similar functionality. In the case of 'post' systems, in contrast, the biometric data have already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned.

---

35 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

36 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39)

37 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive) (OJ L 119, 4.5.2016, p. 89).

(9) For the purposes of this Regulation the notion of publicly accessible space should be understood as referring to any physical place that is accessible to the public, irrespective of whether the place in question is privately or publicly owned. Therefore, the notion does not cover places that are private in nature and normally not freely accessible for third parties, including law enforcement authorities, unless those parties have been specifically invited or authorised, such as homes, private clubs, offices, warehouses and factories. Online spaces are not covered either, as they are not physical spaces. However, the mere fact that certain conditions for accessing a particular space may apply, such as admission tickets or age restrictions, does not mean that the space is not publicly accessible within the meaning of this Regulation. Consequently, in addition to public spaces such as streets, relevant parts of government buildings and most transport infrastructure, spaces such as cinemas, theatres, shops and shopping centres are normally also publicly accessible. Whether a given space is accessible to the public should however be determined on a case-by-case basis, having regard to the specificities of the individual situation at hand.

(10) In order to ensure a level playing field and an effective protection of rights and freedoms of individuals across the Union, the rules established by this Regulation should apply to providers of AI systems in a non-discriminatory manner, irrespective of whether they are established within the Union or in a third country, and to users of AI systems established within the Union.

(11) In light of their digital nature, certain AI systems should fall within the scope of this Regulation even when they are neither placed on the market, nor put into service, nor used in the Union. This is the case for example of an operator established in the Union that contracts certain services to an operator established outside the Union in relation to an activity to be performed by an AI system that would qualify as high-risk and whose effects impact natural persons located in the Union. In those circumstances, the AI system used by the operator outside the Union could process data lawfully collected in and transferred from the Union, and provide to the contracting operator in the Union the output of that AI system resulting from that processing, without that AI system being placed on the market, put into service or used in the Union. To prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union, this Regulation should also apply to providers and users of AI systems that are established in a third country, to the extent the output produced by those systems is used in the Union. Nonetheless, to take into account existing arrangements and special needs for cooperation with foreign partners with whom information and evidence is exchanged, this Regulation should not apply to public authorities of a third country and international organisations when acting in the framework of international agreements concluded at national or European level for law enforcement and judicial cooperation with the Union or with its Member States. Such agreements have been concluded bilaterally between Member States and third countries or between the European Union, Europol and other EU agencies and third countries and international organisations.

(12) This Regulation should also apply to Union institutions, offices, bodies and agencies when acting as a provider or user of an AI system. AI systems exclusively developed or used for military purposes should be excluded from the scope of this Regulation where that use falls under the exclusive remit of the Common Foreign and Security Policy regulated under Title V of the Treaty on the European Union (TEU). This Regulation should be without prejudice to the provisions regarding the liability of

intermediary service providers set out in Directive 2000/31/EC of the European Parliament and of the Council [as amended by the Digital Services Act].

(13) In order to ensure a consistent and high level of protection of public interests as regards health, safety and fundamental rights, common normative standards for all high-risk AI systems should be established. Those standards should be consistent with the Charter of fundamental rights of the European Union (the Charter) and should be non-discriminatory and in line with the Union's international trade commitments.

(14) In order to introduce a proportionate and effective set of binding rules for AI systems, a clearly defined risk-based approach should be followed. That approach should tailor the type and content of such rules to the intensity and scope of the risks that AI systems can generate. It is therefore necessary to prohibit certain artificial intelligence practices, to lay down requirements for high-risk AI systems and obligations for the relevant operators, and to lay down transparency obligations for certain AI systems.

(15) Aside from the many beneficial uses of artificial intelligence, that technology can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices. Such practices are particularly harmful and should be prohibited because they contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and Union fundamental rights, including the right to non-discrimination, data protection and privacy and the rights of the child.

(16) The placing on the market, putting into service or use of certain AI systems intended to distort human behaviour, whereby physical or psychological harms are likely to occur, should be forbidden. Such AI systems deploy subliminal components individuals cannot perceive or exploit vulnerabilities of children and people due to their age, physical or mental incapacities. They do so with the intention to materially distort the behaviour of a person and in a manner that causes or is likely to cause harm to that or another person. The intention may not be presumed if the distortion of human behaviour results from factors external to the AI system which are outside of the control of the provider or the user. Research for legitimate purposes in relation to such AI systems should not be stifled by the prohibition, if such research does not amount to use of the AI system in human-machine relations that exposes natural persons to harm and such research is carried out in accordance with recognised ethical standards for scientific research.

(17) AI systems providing social scoring of natural persons for general purpose by public authorities or on their behalf may lead to discriminatory outcomes and the exclusion of certain groups. They may violate the right to dignity and non-discrimination and the values of equality and justice. Such AI systems evaluate or classify the trustworthiness of natural persons based on their social behaviour in multiple contexts or known or predicted personal or personality characteristics. The social score obtained from such AI systems may lead to the detrimental or unfavourable treatment of natural persons or whole groups thereof in social contexts, which are unrelated to the context in which the data was originally generated or collected or to a detrimental treatment that is disproportionate or unjustified to the gravity of their social behaviour. Such AI systems should be therefore prohibited.

(18) The use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is considered particularly intrusive in the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in 'real-time' carry heightened risks for the rights and freedoms of the persons that are concerned by law enforcement activities.

(19) The use of those systems for the purpose of law enforcement should therefore be prohibited, except in three exhaustively listed and narrowly defined situations, where the use is strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks. Those situations involve the search for potential victims of crime, including missing children; certain threats to the life or physical safety of natural persons or of a terrorist attack; and the detection, localisation, identification or prosecution of perpetrators or suspects of the criminal offences referred to in Council Framework Decision 2002/584/JHA[38] if those criminal offences are punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years and as they are defined in the law of that Member State. Such threshold for the custodial sentence or detention order in accordance with national law contributes to ensure that the offence should be serious enough to potentially justify the use of 'real-time' remote biometric identification systems. Moreover, of the 32 criminal offences listed in the Council Framework Decision 2002/584/JHA, some are in practice likely to be more relevant than others, in that the recourse to 'real-time' remote biometric identification will foreseeably be necessary and proportionate to highly varying degrees for the practical pursuit of the detection, localisation, identification or prosecution of a perpetrator or suspect of the different criminal offences listed and having regard to the likely differences in the seriousness, probability and scale of the harm or possible negative consequences.

(20) In order to ensure that those systems are used in a responsible and proportionate manner, it is also important to establish that, in each of those three exhaustively listed and narrowly defined situations, certain elements should be taken into account, in particular as regards the nature of the situation giving rise to the request and the consequences of the use for the rights and freedoms of all persons concerned and the safeguards and conditions provided for with the use. In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement should be subject to appropriate limits in time and space, having regard in particular to the evidence or indications regarding the threats, the victims or perpetrator. The reference database of persons should be appropriate for each use case in each of the three situations mentioned above.

(21) Each use of a 'real-time' remote biometric identification system in publicly accessible spaces for the purpose of law enforcement should be subject to an express and specific authorisation by a judicial authority or by an independent administrative authority of a Member State. Such authorisation should in principle be obtained prior to the use,

[38] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

except in duly justified situations of urgency, that is, situations where the need to use the systems in question is such as to make it effectively and objectively impossible to obtain an authorisation before commencing the use. In such situations of urgency, the use should be restricted to the absolute minimum necessary and be subject to appropriate safeguards and conditions, as determined in national law and specified in the context of each individual urgent use case by the law enforcement authority itself. In addition, the law enforcement authority should in such situations seek to obtain an authorisation as soon as possible, whilst providing the reasons for not having been able to request it earlier.

(22) Furthermore, it is appropriate to provide, within the exhaustive framework set by this Regulation that such use in the territory of a Member State in accordance with this Regulation should only be possible where and in as far as the Member State in question has decided to expressly provide for the possibility to authorise such use in its detailed rules of national law. Consequently, Member States remain free under this Regulation not to provide for such a possibility at all or to only provide for such a possibility in respect of some of the objectives capable of justifying authorised use identified in this Regulation.

(23) The use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement necessarily involves the processing of biometric data. The rules of this Regulation that prohibit, subject to certain exceptions, such use, which are based on Article 16 TFEU, should apply as *lex specialis* in respect of the rules on the processing of biometric data contained in Article 10 of Directive (EU) 2016/680, thus regulating such use and the processing of biometric data involved in an exhaustive manner. Therefore, such use and processing should only be possible in as far as it is compatible with the framework set by this Regulation, without there being scope, outside that framework, for the competent authorities, where they act for purpose of law enforcement, to use such systems and process such data in connection thereto on the grounds listed in Article 10 of Directive (EU) 2016/680. In this context, this Regulation is not intended to provide the legal basis for the processing of personal data under Article 8 of Directive 2016/680. However, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for purposes other than law enforcement, including by competent authorities, should not be covered by the specific framework regarding such use for the purpose of law enforcement set by this Regulation. Such use for purposes other than law enforcement should therefore not be subject to the requirement of an authorisation under this Regulation and the applicable detailed rules of national law that may give effect to it.

(24) Any processing of biometric data and other personal data involved in the use of AI systems for biometric identification, other than in connection to the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement as regulated by this Regulation, including where those systems are used by competent authorities in publicly accessible spaces for other purposes than law enforcement, should continue to comply with all requirements resulting from Article 9(1) of Regulation (EU) 2016/679, Article 10(1) of Regulation (EU) 2018/1725 and Article 10 of Directive (EU) 2016/680, as applicable.

(25) In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as

annexed to the TEU and to the TFEU, Ireland is not bound by the rules laid down in Article 5(1), point (d), (2) and (3) of this Regulation adopted on the basis of Article 16 of the TFEU which relate to the processing of personal data by the Member States when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU, where Ireland is not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 of the TFEU.

(26) In accordance with Articles 2 and 2a of Protocol No 22 on the position of Denmark, annexed to the TEU and TFEU, Denmark is not bound by rules laid down in Article 5(1), point (d), (2) and (3) of this Regulation adopted on the basis of Article 16 of the TFEU, or subject to their application, which relate to the processing of personal data by the Member States when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU.

(27) High-risk AI systems should only be placed on the Union market or put into service if they comply with certain mandatory requirements. Those requirements should ensure that high-risk AI systems available in the Union or whose output is otherwise used in the Union do not pose unacceptable risks to important Union public interests as recognised and protected by Union law. AI systems identified as high-risk should be limited to those that have a significant harmful impact on the health, safety and fundamental rights of persons in the Union and such limitation minimises any potential restriction to international trade, if any.

(28) AI systems could produce adverse outcomes to health and safety of persons, in particular when such systems operate as components of products. Consistently with the objectives of Union harmonisation legislation to facilitate the free movement of products in the internal market and to ensure that only safe and otherwise compliant products find their way into the market, it is important that the safety risks that may be generated by a product as a whole due to its digital components, including AI systems, are duly prevented and mitigated. For instance, increasingly autonomous robots, whether in the context of manufacturing or personal assistance and care should be able to safely operate and performs their functions in complex environments. Similarly, in the health sector where the stakes for life and health are particularly high, increasingly sophisticated diagnostics systems and systems supporting human decisions should be reliable and accurate. The extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high-risk. Those rights include the right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, and non-discrimination, consumer protection, workers' rights, rights of persons with disabilities, right to an effective remedy and to a fair trial, right of defence and the presumption of innocence, right to good administration. In addition to those rights, it is important to highlight that children have specific rights as enshrined in Article 24 of the EU Charter and in the United Nations Convention on the Rights of the Child (further elaborated in the UNCRC General Comment No. 25 as regards the digital environment), both of which require consideration of the children's vulnerabilities and provision of such protection and care as necessary for their well-being. The fundamental right to a high level of environmental protection enshrined in the Charter and implemented in Union policies should also be considered when assessing the severity of the harm that an AI system can cause, including in relation to the health and safety of persons.

(29) As regards high-risk AI systems that are safety components of products or systems, or which are themselves products or systems falling within the scope of Regulation (EC) No 300/2008 of the European Parliament and of the Council[39], Regulation (EU) No 167/2013 of the European Parliament and of the Council[40], Regulation (EU) No 168/2013 of the European Parliament and of the Council[41], Directive 2014/90/EU of the European Parliament and of the Council[42], Directive (EU) 2016/797 of the European Parliament and of the Council[43], Regulation (EU) 2018/858 of the European Parliament and of the Council[44], Regulation (EU) 2018/1139 of the European Parliament and of the Council[45], and Regulation (EU) 2019/2144 of the European Parliament and of the Council[46], it is appropriate to amend those acts to ensure that the Commission takes into account, on the basis of the technical and regulatory specificities of each sector, and without interfering with existing governance, conformity assessment and enforcement mechanisms and authorities established therein, the mandatory requirements for high-risk AI systems laid down in this Regulation when adopting any relevant future delegated or implementing acts on the basis of those acts.

(30) As regards AI systems that are safety components of products, or which are themselves products, falling within the scope of certain Union harmonisation legislation, it is appropriate to classify them as high-risk under this Regulation if the product in question undergoes the conformity assessment procedure with a third-party conformity assessment body pursuant to that relevant Union harmonisation legislation.

---

39 Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

40 Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles (OJ L 60, 2.3.2013, p. 1).

41 Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles (OJ L 60, 2.3.2013, p. 52).

42 Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146).

43 Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (OJ L 138, 26.5.2016, p. 44).

44 Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (OJ L 151, 14.6.2018, p. 1).

45 Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).

46 Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1).

In particular, such products are machinery, toys, lifts, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, recreational craft equipment, cableway installations, appliances burning gaseous fuels, medical devices, and in vitro diagnostic medical devices.

(31) The classification of an AI system as high-risk pursuant to this Regulation should not necessarily mean that the product whose safety component is the AI system, or the AI system itself as a product, is considered 'high-risk' under the criteria established in the relevant Union harmonisation legislation that applies to the product. This is notably the case for Regulation (EU) 2017/745 of the European Parliament and of the Council[47] and Regulation (EU) 2017/746 of the European Parliament and of the Council[48], where a third-party conformity assessment is provided for medium-risk and high-risk products.

(32) As regards stand-alone AI systems, meaning high-risk AI systems other than those that are safety components of products, or which are themselves products, it is appropriate to classify them as high-risk if, in the light of their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence and they are used in a number of specifically pre-defined areas specified in the Regulation. The identification of those systems is based on the same methodology and criteria envisaged also for any future amendments of the list of high-risk AI systems.

(33) Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. This is particularly relevant when it comes to age, ethnicity, sex or disabilities. Therefore, 'real-time' and 'post' remote biometric identification systems should be classified as high-risk. In view of the risks that they pose, both types of remote biometric identification systems should be subject to specific requirements on logging capabilities and human oversight.

(34) As regards the management and operation of critical infrastructure, it is appropriate to classify as high-risk the AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity, since their failure or malfunctioning may put at risk the life and health of persons at large scale and lead to appreciable disruptions in the ordinary conduct of social and economic activities.

(35) AI systems used in education or vocational training, notably for determining access or assigning persons to educational and vocational training institutions or to evaluate persons on tests as part of or as a precondition for their education should be considered high-risk, since they may determine the educational and professional course of a person's life and therefore affect their ability to secure their livelihood. When improperly designed and used, such systems may violate the right to education and

---

47 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).

48 Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

training as well as the right not to be discriminated against and perpetuate historical patterns of discrimination.

(36) AI systems used in employment, workers management and access to self-employment, notably for the recruitment and selection of persons, for making decisions on promotion and termination and for task allocation, monitoring or evaluation of persons in work-related contractual relationships, should also be classified as high-risk, since those systems may appreciably impact future career prospects and livelihoods of these persons. Relevant work-related contractual relationships should involve employees and persons providing services through platforms as referred to in the Commission Work Programme 2021. Such persons should in principle not be considered users within the meaning of this Regulation. Throughout the recruitment process and in the evaluation, promotion, or retention of persons in work-related contractual relationships, such systems may perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation. AI systems used to monitor the performance and behaviour of these persons may also impact their rights to data protection and privacy.

(37) Another area in which the use of AI systems deserves special consideration is the access to and enjoyment of certain essential private and public services and benefits necessary for people to fully participate in society or to improve one's standard of living. In particular, AI systems used to evaluate the credit score or creditworthiness of natural persons should be classified as high-risk AI systems, since they determine those persons' access to financial resources or essential services such as housing, electricity, and telecommunication services. AI systems used for this purpose may lead to discrimination of persons or groups and perpetuate historical patterns of discrimination, for example based on racial or ethnic origins, disabilities, age, sexual orientation, or create new forms of discriminatory impacts. Considering the very limited scale of the impact and the available alternatives on the market, it is appropriate to exempt AI systems for the purpose of creditworthiness assessment and credit scoring when put into service by small-scale providers for their own use. Natural persons applying for or receiving public assistance benefits and services from public authorities are typically dependent on those benefits and services and in a vulnerable position in relation to the responsible authorities. If AI systems are used for determining whether such benefits and services should be denied, reduced, revoked or reclaimed by authorities, they may have a significant impact on persons' livelihood and may infringe their fundamental rights, such as the right to social protection, non-discrimination, human dignity or an effective remedy. Those systems should therefore be classified as high-risk. Nonetheless, this Regulation should not hamper the development and use of innovative approaches in the public administration, which would stand to benefit from a wider use of compliant and safe AI systems, provided that those systems do not entail a high risk to legal and natural persons. Finally, AI systems used to dispatch or establish priority in the dispatching of emergency first response services should also be classified as high-risk since they make decisions in very critical situations for the life and health of persons and their property.

(38) Actions by law enforcement authorities involving certain uses of AI systems are characterised by a significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights guaranteed in the Charter. In particular, if the AI system is not

trained with high quality data, does not meet adequate requirements in terms of its accuracy or robustness, or is not properly designed and tested before being put on the market or otherwise put into service, it may single out people in a discriminatory or otherwise incorrect or unjust manner. Furthermore, the exercise of important procedural fundamental rights, such as the right to an effective remedy and to a fair trial as well as the right of defence and the presumption of innocence, could be hampered, in particular, where such AI systems are not sufficiently transparent, explainable and documented. It is therefore appropriate to classify as high-risk a number of AI systems intended to be used in the law enforcement context where accuracy, reliability and transparency is particularly important to avoid adverse impacts, retain public trust and ensure accountability and effective redress. In view of the nature of the activities in question and the risks relating thereto, those high-risk AI systems should include in particular AI systems intended to be used by law enforcement authorities for individual risk assessments, polygraphs and similar tools or to detect the emotional state of natural person, to detect 'deep fakes', for the evaluation of the reliability of evidence in criminal proceedings, for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons, or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups, for profiling in the course of detection, investigation or prosecution of criminal offences, as well as for crime analytics regarding natural persons. AI systems specifically intended to be used for administrative proceedings by tax and customs authorities should not be considered high-risk AI systems used by law enforcement authorities for the purposes of prevention, detection, investigation and prosecution of criminal offences.

(39) AI systems used in migration, asylum and border control management affect people who are often in particularly vulnerable position and who are dependent on the outcome of the actions of the competent public authorities. The accuracy, non-discriminatory nature and transparency of the AI systems used in those contexts are therefore particularly important to guarantee the respect of the fundamental rights of the affected persons, notably their rights to free movement, non-discrimination, protection of private life and personal data, international protection and good administration. It is therefore appropriate to classify as high-risk AI systems intended to be used by the competent public authorities charged with tasks in the fields of migration, asylum and border control management as polygraphs and similar tools or to detect the emotional state of a natural person; for assessing certain risks posed by natural persons entering the territory of a Member State or applying for visa or asylum; for verifying the authenticity of the relevant documents of natural persons; for assisting competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the objective to establish the eligibility of the natural persons applying for a status. AI systems in the area of migration, asylum and border control management covered by this Regulation should comply with the relevant procedural requirements set by the Directive 2013/32/EU of the European Parliament and of the Council[49], the Regulation (EC) No

[49] Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (OJ L 180, 29.6.2013, p. 60).

810/2009 of the European Parliament and of the Council[50] and other relevant legislation.

(40) Certain AI systems intended for the administration of justice and democratic processes should be classified as high-risk, considering their potentially significant impact on democracy, rule of law, individual freedoms as well as the right to an effective remedy and to a fair trial. In particular, to address the risks of potential biases, errors and opacity, it is appropriate to qualify as high-risk AI systems intended to assist judicial authorities in researching and interpreting facts and the law and in applying the law to a concrete set of facts. Such qualification should not extend, however, to AI systems intended for purely ancillary administrative activities that do not affect the actual administration of justice in individual cases, such as anonymisation or pseudonymisation of judicial decisions, documents or data, communication between personnel, administrative tasks or allocation of resources.

(41) The fact that an AI system is classified as high risk under this Regulation should not be interpreted as indicating that the use of the system is necessarily lawful under other acts of Union law or under national law compatible with Union law, such as on the protection of personal data, on the use of polygraphs and similar tools or other systems to detect the emotional state of natural persons. Any such use should continue to occur solely in accordance with the applicable requirements resulting from the Charter and from the applicable acts of secondary Union law and national law. This Regulation should not be understood as providing for the legal ground for processing of personal data, including special categories of personal data, where relevant.

(42) To mitigate the risks from high-risk AI systems placed or otherwise put into service on the Union market for users and affected persons, certain mandatory requirements should apply, taking into account the intended purpose of the use of the system and according to the risk management system to be established by the provider.

(43) Requirements should apply to high-risk AI systems as regards the quality of data sets used, technical documentation and record-keeping, transparency and the provision of information to users, human oversight, and robustness, accuracy and cybersecurity. Those requirements are necessary to effectively mitigate the risks for health, safety and fundamental rights, as applicable in the light of the intended purpose of the system, and no other less trade restrictive measures are reasonably available, thus avoiding unjustified restrictions to trade.

(44) High data quality is essential for the performance of many AI systems, especially when techniques involving the training of models are used, with a view to ensure that the high-risk AI system performs as intended and safely and it does not become the source of discrimination prohibited by Union law. High quality training, validation and testing data sets require the implementation of appropriate data governance and management practices. Training, validation and testing data sets should be sufficiently relevant, representative and free of errors and complete in view of the intended purpose of the system. They should also have the appropriate statistical properties, including as regards the persons or groups of persons on which the high-risk AI

[50] Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) (OJ L 243, 15.9.2009, p. 1).

system is intended to be used. In particular, training, validation and testing data sets should take into account, to the extent required in the light of their intended purpose, the features, characteristics or elements that are particular to the specific geographical, behavioural or functional setting or context within which the AI system is intended to be used. In order to protect the right of others from the discrimination that might result from the bias in AI systems, the providers shouldbe able to process also special categories of personal data, as a matter of substantial public interest, in order to ensure the bias monitoring, detection and correction in relation to high-risk AI systems.

(45) For the development of high-risk AI systems, certain actors, such as providers, notified bodies and other relevant entities, such as digital innovation hubs, testing experimentation facilities and researchers, should be able to access and use high quality datasets within their respective fields of activities which are related to this Regulation. European common data spaces established by the Commission and the facilitation of data sharing between businesses and with government in the public interest will be instrumental to provide trustful, accountable and non-discriminatory access to high quality data for the training, validation and testing of AI systems. For example, in health, the European health data space will facilitate non-discriminatory access to health data and the training of artificial intelligence algorithms on those datasets, in a privacy-preserving, secure, timely, transparent and trustworthy manner, and with an appropriate institutional governance. Relevant competent authorities, including sectoral ones, providing or supporting the access to data may also support the provision of high-quality data for the training, validation and testing of AI systems.

(46) Having information on how high-risk AI systems have been developed and how they perform throughout their lifecycle is essential to verify compliance with the requirements under this Regulation. This requires keeping records and the availability of a technical documentation, containing information which is necessary to assess the compliance of the AI system with the relevant requirements. Such information should include the general characteristics, capabilities and limitations of the system, algorithms, data, training, testing and validation processes used as well as documentation on the relevant risk management system. The technical documentation should be kept up to date.

(47) To address the opacity that may make certain AI systems incomprehensible to or too complex for natural persons, a certain degree of transparency should be required for high-risk AI systems. Users should be able to interpret the system output and use it appropriately. High-risk AI systems should therefore be accompanied by relevant documentation and instructions of use and include concise and clear information, including in relation to possible risks to fundamental rights and discrimination, where appropriate.

(48) High-risk AI systems should be designed and developed in such a way that natural persons can oversee their functioning. For this purpose, appropriate human oversight measures should be identified by the provider of the system before its placing on the market or putting into service. In particular, where appropriate, such measures should guarantee that the system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human operator, and that the natural persons to whom human oversight has been assigned have the necessary competence, training and authority to carry out that role.

(49) High-risk AI systems should perform consistently throughout their lifecycle and meet an appropriate level of accuracy, robustness and cybersecurity in accordance with the generally acknowledged state of the art. The level of accuracy and accuracy metrics should be communicated to the users.

(50) The technical robustness is a key requirement for high-risk AI systems. They should be resilient against risks connected to the limitations of the system (e.g. errors, faults, inconsistencies, unexpected situations) as well as against malicious actions that may compromise the security of the AI system and result in harmful or otherwise undesirable behaviour. Failure to protect against these risks could lead to safety impacts or negatively affect the fundamental rights, for example due to erroneous decisions or wrong or biased outputs generated by the AI system.

(51) Cybersecurity plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behaviour, performance or compromise their security properties by malicious third parties exploiting the system's vulnerabilities. Cyberattacks against AI systems can leverage AI specific assets, such as training data sets (e.g. data poisoning) or trained models (e.g. adversarial attacks), or exploit vulnerabilities in the AI system's digital assets or the underlying ICT infrastructure. To ensure a level of cybersecurity appropriate to the risks, suitable measures should therefore be taken by the providers of high-risk AI systems, also taking into account as appropriate the underlying ICT infrastructure.

(52) As part of Union harmonisation legislation, rules applicable to the placing on the market, putting into service and use of high-risk AI systems should be laid down consistently with Regulation (EC) No 765/2008 of the European Parliament and of the Council[51] setting out the requirements for accreditation and the market surveillance of products, Decision No 768/2008/EC of the European Parliament and of the Council[52] on a common framework for the marketing of products and Regulation (EU) 2019/1020 of the European Parliament and of the Council[53] on market surveillance and compliance of products ('New Legislative Framework for the marketing of products').

(53) It is appropriate that a specific natural or legal person, defined as the provider, takes the responsibility for the placing on the market or putting into service of a high-risk AI system, regardless of whether that natural or legal person is the person who designed or developed the system.

(54) The provider should establish a sound quality management system, ensure the accomplishment of the required conformity assessment procedure, draw up the relevant documentation and establish a robust post-market monitoring system. Public authorities which put into service high-risk AI systems for their own use may adopt

---

51 Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

52 Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).

53 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance) (OJ L 169, 25.6.2019, p. 1–44).

and implement the rules for the quality management system as part of the quality management system adopted at a national or regional level, as appropriate, taking into account the specificities of the sector and the competences and organisation of the public authority in question.

(55) Where a high-risk AI system that is a safety component of a product which is covered by a relevant New Legislative Framework sectorial legislation is not placed on the market or put into service independently from the product, the manufacturer of the final product as defined under the relevant New Legislative Framework legislation should comply with the obligations of the provider established in this Regulation and notably ensure that the AI system embedded in the final product complies with the requirements of this Regulation.

(56) To enable enforcement of this Regulation and create a level-playing field for operators, and taking into account the different forms of making available of digital products, it is important to ensure that, under all circumstances, a person established in the Union can provide authorities with all the necessary information on the compliance of an AI system. Therefore, prior to making their AI systems available in the Union, where an importer cannot be identified, providers established outside the Union shall, by written mandate, appoint an authorised representative established in the Union.

(57) In line with New Legislative Framework principles, specific obligations for relevant economic operators, such as importers and distributors, should be set to ensure legal certainty and facilitate regulatory compliance by those relevant operators.

(58) Given the nature of AI systems and the risks to safety and fundamental rights possibly associated with their use, including as regard the need to ensure proper monitoring of the performance of an AI system in a real-life setting, it is appropriate to set specific responsibilities for users. Users should in particular use high-risk AI systems in accordance with the instructions of use and certain other obligations should be provided for with regard to monitoring of the functioning of the AI systems and with regard to record-keeping, as appropriate.

(59) It is appropriate to envisage that the user of the AI system should be the natural or legal person, public authority, agency or other body under whose authority the AI system is operated except where the use is made in the course of a personal non-professional activity.

(60) In the light of the complexity of the artificial intelligence value chain, relevant third parties, notably the ones involved in the sale and the supply of software, software tools and components, pre-trained models and data, or providers of network services, should cooperate, as appropriate, with providers and users to enable their compliance with the obligations under this Regulation and with competent authorities established under this Regulation.

(61) Standardisation should play a key role to provide technical solutions to providers to ensure compliance with this Regulation. Compliance with harmonised standards as defined in Regulation (EU) No 1025/2012 of the European Parliament and of the

Council[54] should be a means for providers to demonstrate conformity with the requirements of this Regulation. However, the Commission could adopt common technical specifications in areas where no harmonised standards exist or where they are insufficient.

(62) In order to ensure a high level of trustworthiness of high-risk AI systems, those systems should be subject to a conformity assessment prior to their placing on the market or putting into service.

(63) It is appropriate that, in order to minimise the burden on operators and avoid any possible duplication, for high-risk AI systems related to products which are covered by existing Union harmonisation legislation following the New Legislative Framework approach, the compliance of those AI systems with the requirements of this Regulation should be assessed as part of the conformity assessment already foreseen under that legislation. The applicability of the requirements of this Regulation should thus not affect the specific logic, methodology or general structure of conformity assessment under the relevant specific New Legislative Framework legislation. This approach is fully reflected in the interplay between this Regulation and the [Machinery Regulation]. While safety risks of AI systems ensuring safety functions in machinery are addressed by the requirements of this Regulation, certain specific requirements in the [Machinery Regulation] will ensure the safe integration of the AI system into the overall machinery, so as not to compromise the safety of the machinery as a whole. The [Machinery Regulation] applies the same definition of AI system as this Regulation.

(64) Given the more extensive experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate to limit, at least in an initial phase of application of this Regulation, the scope of application of third-party conformity assessment for high-risk AI systems other than those related to products. Therefore, the conformity assessment of such systems should be carried out as a general rule by the provider under its own responsibility, with the only exception of AI systems intended to be used for the remote biometric identification of persons, for which the involvement of a notified body in the conformity assessment should be foreseen, to the extent they are not prohibited.

(65) In order to carry out third-party conformity assessment for AI systems intended to be used for the remote biometric identification of persons, notified bodies should be designated under this Regulation by the national competent authorities, provided they are compliant with a set of requirements, notably on independence, competence and absence of conflicts of interests.

(66) In line with the commonly established notion of substantial modification for products regulated by Union harmonisation legislation, it is appropriate that an AI system undergoes a new conformity assessment whenever a change occurs which may affect

[54] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

the compliance of the system with this Regulation or when the intended purpose of the system changes. In addition, as regards AI systems which continue to 'learn' after being placed on the market or put into service (i.e. they automatically adapt how functions are carried out), it is necessary to provide rules establishing that changes to the algorithm and its performance that have been pre-determined by the provider and assessed at the moment of the conformity assessment should not constitute a substantial modification.

(67) High-risk AI systems should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. Member States should not create unjustified obstacles to the placing on the market or putting into service of high-risk AI systems that comply with the requirements laid down in this Regulation and bear the CE marking.

(68) Under certain conditions, rapid availability of innovative technologies may be crucial for health and safety of persons and for society as a whole. It is thus appropriate that under exceptional reasons of public security or protection of life and health of natural persons and the protection of industrial and commercial property, Member States could authorise the placing on the market or putting into service of AI systems which have not undergone a conformity assessment.

(69) In order to facilitate the work of the Commission and the Member States in the artificial intelligence field as well as to increase the transparency towards the public, providers of high-risk AI systems other than those related to products falling within the scope of relevant existing Union harmonisation legislation, should be required to register their high-risk AI system in a EU database, to be established and managed by the Commission. The Commission should be the controller of that database, in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council[55]. In order to ensure the full functionality of the database, when deployed, the procedure for setting the database should include the elaboration of functional specifications by the Commission and an independent audit report.

(70) Certain AI systems intended to interact with natural persons or to generate content may pose specific risks of impersonation or deception irrespective of whether they qualify as high-risk or not. In certain circumstances, the use of these systems should therefore be subject to specific transparency obligations without prejudice to the requirements and obligations for high-risk AI systems. In particular, natural persons should be notified that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use. Moreover, natural persons should be notified when they are exposed to an emotion recognition system or a biometric categorisation system. Such information and notifications should be provided in accessible formats for persons with disabilities. Further, users, who use an AI system to generate or manipulate image, audio or video content that appreciably resembles existing persons, places or events and would falsely appear to a person to be authentic, should disclose that the content has been artificially created or manipulated by

[55] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

labelling the artificial intelligence output accordingly and disclosing its artificial origin.

(71) Artificial intelligence is a rapidly developing family of technologies that requires novel forms of regulatory oversight and a safe space for experimentation, while ensuring responsible innovation and integration of appropriate safeguards and risk mitigation measures. To ensure a legal framework that is innovation-friendly, future-proof and resilient to disruption, national competent authorities from one or more Member States should be encouraged to establish artificial intelligence regulatory sandboxes to facilitate the development and testing of innovative AI systems under strict regulatory oversight before these systems are placed on the market or otherwise put into service.

(72) The objectives of the regulatory sandboxes should be to foster AI innovation by establishing a controlled experimentation and testing environment in the development and pre-marketing phase with a view to ensuring compliance of the innovative AI systems with this Regulation and other relevant Union and Member States legislation; to enhance legal certainty for innovators and the competent authorities' oversight and understanding of the opportunities, emerging risks and the impacts of AI use, and to accelerate access to markets, including by removing barriers for small and medium enterprises (SMEs) and start-ups. To ensure uniform implementation across the Union and economies of scale, it is appropriate to establish common rules for the regulatory sandboxes' implementation and a framework for cooperation between the relevant authorities involved in the supervision of the sandboxes. This Regulation should provide the legal basis for the use of personal data collected for other purposes for developing certain AI systems in the public interest within the AI regulatory sandbox, in line with Article 6(4) of Regulation (EU) 2016/679, and Article 6 of Regulation (EU) 2018/1725, and without prejudice to Article 4(2) of Directive (EU) 2016/680. Participants in the sandbox should ensure appropriate safeguards and cooperate with the competent authorities, including by following their guidance and acting expeditiously and in good faith to mitigate any high-risks to safety and fundamental rights that may arise during the development and experimentation in the sandbox. The conduct of the participants in the sandbox should be taken into account when competent authorities decide whether to impose an administrative fine under Article 83(2) of Regulation 2016/679 and Article 57 of Directive 2016/680.

(73) In order to promote and protect innovation, it is important that the interests of small-scale providers and users of AI systems are taken into particular account. To this objective, Member States should develop initiatives, which are targeted at those operators, including on awareness raising and information communication. Moreover, the specific interests and needs of small-scale providers shall be taken into account when Notified Bodies set conformity assessment fees. Translation costs related to mandatory documentation and communication with authorities may constitute a significant cost for providers and other operators, notably those of a smaller scale. Member States should possibly ensure that one of the languages determined and accepted by them for relevant providers' documentation and for communication with operators is one which is broadly understood by the largest possible number of cross-border users.

(74) In order to minimise the risks to implementation resulting from lack of knowledge and expertise in the market as well as to facilitate compliance of providers and notified

bodies with their obligations under this Regulation, the AI-on demand platform, the European Digital Innovation Hubs and the Testing and Experimentation Facilities established by the Commission and the Member States at national or EU level should possibly contribute to the implementation of this Regulation. Within their respective mission and fields of competence, they may provide in particular technical and scientific support to providers and notified bodies.

(75) It is appropriate that the Commission facilitates, to the extent possible, access to Testing and Experimentation Facilities to bodies, groups or laboratories established or accredited pursuant to any relevant Union harmonisation legislation and which fulfil tasks in the context of conformity assessment of products or devices covered by that Union harmonisation legislation. This is notably the case for expert panels, expert laboratories and reference laboratories in the field of medical devices pursuant to Regulation (EU) 2017/745 and Regulation (EU) 2017/746.

(76) In order to facilitate a smooth, effective and harmonised implementation of this Regulation a European Artificial Intelligence Board should be established. The Board should be responsible for a number of advisory tasks, including issuing opinions, recommendations, advice or guidance on matters related to the implementation of this Regulation, including on technical specifications or existing standards regarding the requirements established in this Regulation and providing advice to and assisting the Commission on specific questions related to artificial intelligence.

(77) Member States hold a key role in the application and enforcement of this Regulation. In this respect, each Member State should designate one or more national competent authorities for the purpose of supervising the application and implementation of this Regulation. In order to increase organisation efficiency on the side of Member States and to set an official point of contact vis-à-vis the public and other counterparts at Member State and Union levels, in each Member State one national authority should be designated as national supervisory authority.

(78) In order to ensure that providers of high-risk AI systems can take into account the experience on the use of high-risk AI systems for improving their systems and the design and development process or can take any possible corrective action in a timely manner, all providers should have a post-market monitoring system in place. This system is also key to ensure that the possible risks emerging from AI systems which continue to 'learn' after being placed on the market or put into service can be more efficiently and timely addressed. In this context, providers should also be required to have a system in place to report to the relevant authorities any serious incidents or any breaches to national and Union law protecting fundamental rights resulting from the use of their AI systems.

(79) In order to ensure an appropriate and effective enforcement of the requirements and obligations set out by this Regulation, which is Union harmonisation legislation, the system of market surveillance and compliance of products established by Regulation (EU) 2019/1020 should apply in its entirety. Where necessary for their mandate, national public authorities or bodies, which supervise the application of Union law protecting fundamental rights, including equality bodies, should also have access to any documentation created under this Regulation.

(80) Union legislation on financial services includes internal governance and risk management rules and requirements which are applicable to regulated financial institutions in the course of provision of those services, including when they make use of AI systems. In order to ensure coherent application and enforcement of the obligations under this Regulation and relevant rules and requirements of the Union financial services legislation, the authorities responsible for the supervision and enforcement of the financial services legislation, including where applicable the European Central Bank, should be designated as competent authorities for the purpose of supervising the implementation of this Regulation, including for market surveillance activities, as regards AI systems provided or used by regulated and supervised financial institutions. To further enhance the consistency between this Regulation and the rules applicable to credit institutions regulated under Directive 2013/36/EU of the European Parliament and of the Council[56], it is also appropriate to integrate the conformity assessment procedure and some of the providers' procedural obligations in relation to risk management, post marketing monitoring and documentation into the existing obligations and procedures under Directive 2013/36/EU. In order to avoid overlaps, limited derogations should also be envisaged in relation to the quality management system of providers and the monitoring obligation placed on users of high-risk AI systems to the extent that these apply to credit institutions regulated by Directive 2013/36/EU.

(81) The development of AI systems other than high-risk AI systems in accordance with the requirements of this Regulation may lead to a larger uptake of trustworthy artificial intelligence in the Union. Providers of non-high-risk AI systems should be encouraged to create codes of conduct intended to foster the voluntary application of the mandatory requirements applicable to high-risk AI systems. Providers should also be encouraged to apply on a voluntary basis additional requirements related, for example, to environmental sustainability, accessibility to persons with disability, stakeholders' participation in the design and development of AI systems, and diversity of the development teams. The Commission may develop initiatives, including of a sectorial nature, to facilitate the lowering of technical barriers hindering cross-border exchange of data for AI development, including on data access infrastructure, semantic and technical interoperability of different types of data.

(82) It is important that AI systems related to products that are not high-risk in accordance with this Regulation and thus are not required to comply with the requirements set out herein are nevertheless safe when placed on the market or put into service. To contribute to this objective, the Directive 2001/95/EC of the European Parliament and of the Council[57] would apply as a safety net.

(83) In order to ensure trustful and constructive cooperation of competent authorities on Union and national level, all parties involved in the application of this Regulation should respect the confidentiality of information and data obtained in carrying out their tasks.

---

56 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

57 Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 11, 15.1.2002, p. 4).

(84) Member States should take all necessary measures to ensure that the provisions of this Regulation are implemented, including by laying down effective, proportionate and dissuasive penalties for their infringement. For certain specific infringements, Member States should take into account the margins and criteria set out in this Regulation. The European Data Protection Supervisor should have the power to impose fines on Union institutions, agencies and bodies falling within the scope of this Regulation.

(85) In order to ensure that the regulatory framework can be adapted where necessary, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to amend the techniques and approaches referred to in Annex I to define AI systems, the Union harmonisation legislation listed in Annex II, the high-risk AI systems listed in Annex III, the provisions regarding technical documentation listed in Annex IV, the content of the EU declaration of conformity in Annex V, the provisions regarding the conformity assessment procedures in Annex VI and VII and the provisions establishing the high-risk AI systems to which the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation should apply. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[58]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(86) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[59].

(87) Since the objective of this Regulation cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 TEU. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(88) This Regulation should apply from … [*OP – please insert the date established in Art. 85*]. However, the infrastructure related to the governance and the conformity assessment system should be operational before that date, therefore the provisions on notified bodies and governance structure should apply from … [*OP – please insert the date – three months following the entry into force of this Regulation*]. In addition, Member States should lay down and notify to the Commission the rules on penalties, including administrative fines, and ensure that they are properly and effectively implemented by the date of application of this Regulation. Therefore the provisions on

---

58 OJ L 123, 12.5.2016, p. 1.

59 Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p.13).

penalties should apply from [*OP – please insert the date – twelve months following the entry into force of this Regulation*].

(89) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725 and delivered an opinion on […]".

HAVE ADOPTED THIS REGULATION:

# TITLE I

# GENERAL PROVISIONS

*Article 1*
*Subject matter*

This Regulation lays down:

(a) harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union;

(a) prohibitions of certain artificial intelligence practices;

(b) specific requirements for high-risk AI systems and obligations for operators of such systems;

(c) harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content;

(d) rules on market monitoring and surveillance.

*Article 2*
*Scope*

1. This Regulation applies to:

(a) providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country;

(b) users of AI systems located within the Union;

(c) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union;

2. For high-risk AI systems that are safety components of products or systems, or which are themselves products or systems, falling within the scope of the following acts, only Article 84 of this Regulation shall apply:

(a) Regulation (EC) 300/2008;

(b) Regulation (EU) No 167/2013;

(c) Regulation (EU) No 168/2013;

(d) Directive 2014/90/EU;

(e) Directive (EU) 2016/797;

(f) Regulation (EU) 2018/858;

(g) Regulation (EU) 2018/1139;

(h) Regulation (EU) 2019/2144.

3. This Regulation shall not apply to AI systems developed or used exclusively for military purposes.

4. This Regulation shall not apply to public authorities in a third country nor to international organisations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States.

5. This Regulation shall not affect the application of the provisions on the liability of intermediary service providers set out in Chapter II, Section IV of Directive 2000/31/EC of the European Parliament and of the Council[60] [*as to be replaced by the corresponding provisions of the Digital Services Act*].

*Article 3*
*Definitions*

For the purpose of this Regulation, the following definitions apply:

(1) 'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;

(1) 'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge;

[60] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

(3) ‘small-scale provider’ means a provider that is a micro or small enterprise within the meaning of Commission Recommendation 2003/361/EC[61];

(4) ‘user’ means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity;

(5) ‘authorised representative’ means any natural or legal person established in the Union who has received a written mandate from a provider of an AI system to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation;

(6) ‘importer’ means any natural or legal person established in the Union that places on the market or puts into service an AI system that bears the name or trademark of a natural or legal person established outside the Union;

(7) ‘distributor’ means any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market without affecting its properties;

(8) ‘operator’ means the provider, the user, the authorised representative, the importer and the distributor;

(9) ‘placing on the market’ means the first making available of an AI system on the Union market;

(10) ‘making available on the market’ means any supply of an AI system for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge;

(11) ‘putting into service’ means the supply of an AI system for first use directly to the user or for own use on the Union market for its intended purpose;

(12) ‘intended purpose’ means the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;

(13) ‘reasonably foreseeable misuse’ means the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems;

(14) ‘safety component of a product or system’ means a component of a product or of a system which fulfils a safety function for that product or system or the failure or malfunctioning of which endangers the health and safety of persons or property;

(15) ‘instructions for use’ means the information provided by the provider to inform the user of in particular an AI system’s intended purpose and proper use, inclusive of the

[61] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used;

(16) ‘recall of an AI system’ means any measure aimed at achieving the return to the provider of an AI system made available to users;

(17) ‘withdrawal of an AI system’ means any measure aimed at preventing the distribution, display and offer of an AI system;

(18) ‘performance of an AI system’ means the ability of an AI system to achieve its intended purpose;

(19) ‘notifying authority’ means the national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring;

(20) ‘conformity assessment’ means the process of verifying whether the requirements set out in Title III, Chapter 2 of this Regulation relating to an AI system have been fulfilled;

(21) ‘conformity assessment body’ means a body that performs third-party conformity assessment activities, including testing, certification and inspection;

(22) ‘notified body’ means a conformity assessment body designated in accordance with this Regulation and other relevant Union harmonisation legislation;

(23) ‘substantial modification’ means a change to the AI system following its placing on the market or putting into service which affects the compliance of the AI system with the requirements set out in Title III, Chapter 2 of this Regulation or results in a modification to the intended purpose for which the AI system has been assessed;

(24) ‘CE marking of conformity’ (CE marking) means a marking by which a provider indicates that an AI system is in conformity with the requirements set out in Title III, Chapter 2 of this Regulation and other applicable Union legislation harmonising the conditions for the marketing of products (‘Union harmonisation legislation’) providing for its affixing;

(25) ‘post-market monitoring’ means all activities carried out by providers of AI systems to proactively collect and review experience gained from the use of AI systems they place on the market or put into service for the purpose of identifying any need to immediately apply any necessary corrective or preventive actions;

(26) ‘market surveillance authority’ means the national authority carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020;

(27) ‘harmonised standard’ means a European standard as defined in Article 2(1)(c) of Regulation (EU) No 1025/2012;

(28) ‘common specifications’ means a document, other than a standard, containing technical solutions providing a means to, comply with certain requirements and obligations established under this Regulation;

(29) ‘training data’ means data used for training an AI system through fitting its learnable parameters, including the weights of a neural network;

(30) ‘validation data’ means data used for providing an evaluation of the trained AI system and for tuning its non-learnable parameters and its learning process, among other things, in order to prevent overfitting; whereas the validation dataset can be a separate dataset or part of the training dataset, either as a fixed or variable split;

(31) ‘testing data’ means data used for providing an independent evaluation of the trained and validated AI system in order to confirm the expected performance of that system before its placing on the market or putting into service;

(32) ‘input data’ means data provided to or directly acquired by an AI system on the basis of which the system produces an output;

(33) ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(34) ‘emotion recognition system’ means an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data;

(35) ‘biometric categorisation system’ means an AI system for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data;

(36) ‘remote biometric identification system’ means an AI system for the purpose of identifying natural persons at a distance through the comparison of a person’s biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified ;

(37) ‘‘real-time’ remote biometric identification system’ means a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention.

(38) ‘‘post’ remote biometric identification system’ means a remote biometric identification system other than a ‘real-time’ remote biometric identification system;

(39) ‘publicly accessible space’ means any physical place accessible to the public, regardless of whether certain conditions for access may apply;

(40) ‘law enforcement authority’ means:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(41) 'law enforcement' means activities carried out by law enforcement authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(42) 'national supervisory authority' means the authority to which a Member State assigns the responsibility for the implementation and application of this Regulation, for coordinating the activities entrusted to that Member State, for acting as the single contact point for the Commission, and for representing the Member State at the European Artificial Intelligence Board;

(43) 'national competent authority' means the national supervisory authority, the notifying authority and the market surveillance authority;

(44) 'serious incident' means any incident that directly or indirectly leads, might have led or might lead to any of the following:

(a) the death of a person or serious damage to a person's health, to property or the environment,

(b) a serious and irreversible disruption of the management and operation of critical infrastructure.

*Article 4*
*Amendments to Annex I*

The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend the list of techniques and approaches listed in Annex I, in order to update that list to market and technological developments on the basis of characteristics that are similar to the techniques and approaches listed therein.

# TITLE II

# PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES

*Article 5*

1. The following artificial intelligence practices shall be prohibited:

(a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to

materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm;

(b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm;

(c) the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:

(i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;

(ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity;

(d) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:

(i) the targeted search for specific potential victims of crime, including missing children;

(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;

(iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA[62] and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.

2. The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall take into account the following elements:

(a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;

[62] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

(b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations.

3. As regards paragraphs 1, point (d) and 2, each individual use for the purpose of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 4. However, in a duly justified situation of urgency, the use of the system may be commenced without an authorisation and the authorisation may be requested only during or after the use.

The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2.

4. A Member State may decide to provide for the possibility to fully or partially authorise the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement within the limits and under the conditions listed in paragraphs 1, point (d), 2 and 3. That Member State shall lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, point (d), including which of the criminal offences referred to in point (iii) thereof, the competent authorities may be authorised to use those systems for the purpose of law enforcement.

# TITLE III

# HIGH-RISK AI SYSTEMS

## CHAPTER 1

## CLASSIFICATION OF AI SYSTEMS AS HIGH-RISK

*Article 6*
*Classification rules for high-risk AI systems*

1. Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where both of the following conditions are fulfilled:

   (a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;

   (b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II.

2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.

*Article 7*
*Amendments to Annex III*

1. The Commission is empowered to adopt delegated acts in accordance with Article 73 to update the list in Annex III by adding high-risk AI systems where both of the following conditions are fulfilled:

   (a) the AI systems are intended to be used in any of the areas listed in points 1 to 8 of Annex III;

   (b) the AI systems pose a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights, that is, in respect of its severity and probability of occurrence, equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.

2. When assessing for the purposes of paragraph 1 whether an AI system poses a risk of harm to the health and safety or a risk of adverse impact on fundamental rights that is equivalent to or greater than the risk of harm posed by the high-risk AI systems

already referred to in Annex III, the Commission shall take into account the following criteria:

(a) the intended purpose of the AI system;

(b) the extent to which an AI system has been used or is likely to be used;

(c) the extent to which the use of an AI system has already caused harm to the health and safety or adverse impact on the fundamental rights or has given rise to significant concerns in relation to the materialisation of such harm or adverse impact, as demonstrated by reports or documented allegations submitted to national competent authorities;

(d) the potential extent of such harm or such adverse impact, in particular in terms of its intensity and its ability to affect a plurality of persons;

(e) the extent to which potentially harmed or adversely impacted persons are dependent on the outcome produced with an AI system, in particular because for practical or legal reasons it is not reasonably possible to opt-out from that outcome;

(f) the extent to which potentially harmed or adversely impacted persons are in a vulnerable position in relation to the user of an AI system, in particular due to an imbalance of power, knowledge, economic or social circumstances, or age;

(g) the extent to which the outcome produced with an AI system is easily reversible, whereby outcomes having an impact on the health or safety of persons shall not be considered as easily reversible;

(h) the extent to which existing Union legislation provides for:

(i) effective measures of redress in relation to the risks posed by an AI system, with the exclusion of claims for damages;

(ii) effective measures to prevent or substantially minimise those risks.

## CHAPTER 2

## REQUIREMENTS FOR HIGH-RISK AI SYSTEMS

### *Article 8*
### *Compliance with the requirements*

1. High-risk AI systems shall comply with the requirements established in this Chapter.

2. The intended purpose of the high-risk AI system and the risk management system referred to in Article 9 shall be taken into account when ensuring compliance with those requirements.

*Article 9*
*Risk management system*

1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.

2. The risk management system shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. It shall comprise the following steps:

   (a) identification and analysis of the known and foreseeable risks associated with each high-risk AI system;

   (b) estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse;

   (c) evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system referred to in Article 61;

   (d) adoption of suitable risk management measures in accordance with the provisions of the following paragraphs.

3. The risk management measures referred to in paragraph 2, point (d) shall give due consideration to the effects and possible interactions resulting from the combined application of the requirements set out in this Chapter 2. They shall take into account the generally acknowledged state of the art, including as reflected in relevant harmonised standards or common specifications.

4. The risk management measures referred to in paragraph 2, point (d) shall be such that any residual risk associated with each hazard as well as the overall residual risk of the high-risk AI systems is judged acceptable, provided that the high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse. Those residual risks shall be communicated to the user.

   In identifying the most appropriate risk management measures, the following shall be ensured:

   (a) elimination or reduction of risks as far as possible through adequate design and development;

   (b) where appropriate, implementation of adequate mitigation and control measures in relation to risks that cannot be eliminated;

   (c) provision of adequate information pursuant to Article 13, in particular as regards the risks referred to in paragraph 2, point (b) of this Article, and, where appropriate, training to users.

   In eliminating or reducing risks related to the use of the high-risk AI system, due consideration shall be given to the technical knowledge, experience, education, training to be expected by the user and the environment in which the system is intended to be used.

5. High-risk AI systems shall be tested for the purposes of identifying the most appropriate risk management measures. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and they are in compliance with the requirements set out in this Chapter.

6. Testing procedures shall be suitable to achieve the intended purpose of the AI system and do not need to go beyond what is necessary to achieve that purpose.

7. The testing of the high-risk AI systems shall be performed, as appropriate, at any point in time throughout the development process, and, in any event, prior to the placing on the market or the putting into service. Testing shall be made against preliminarily defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.

8. When implementing the risk management system described in paragraphs 1 to 7, specific consideration shall be given to whether the high-risk AI system is likely to be accessed by or have an impact on children.

9. For credit institutions regulated by Directive 2013/36/EU, the aspects described in paragraphs 1 to 8 shall be part of the risk management procedures established by those institutions pursuant to Article 74 of that Directive.

*Article 10*
*Data and data governance*

1. High-risk AI systems which make use of techniques involving the training of models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5.

2. Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular,

   (a) the relevant design choices;

   (b) data collection;

   (c) relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation;

   (d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent;

   (e) a prior assessment of the availability, quantity and suitability of the data sets that are needed;

   (f) examination in view of possible biases;

   (g) the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed.

3. Training, validation and testing data sets shall be relevant, representative, free of errors and complete. They shall have the appropriate statistical properties, including,

where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used. These characteristics of the data sets may be met at the level of individual data sets or a combination thereof.

4. Training, validation and testing data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used.

5. To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.

6. Appropriate data governance and management practices shall apply for the development of high-risk AI systems other than those which make use of techniques involving the training of models in order to ensure that those high-risk AI systems comply with paragraph 2.

*Article 11*
*Technical documentation*

1. The technical documentation of a high-risk AI system shall be drawn up before that system is placed on the market or put into service and shall be kept up-to date.

   The technical documentation shall be drawn up in such a way to demonstrate that the high-risk AI system complies with the requirements set out in this Chapter and provide national competent authorities and notified bodies with all the necessary information to assess the compliance of the AI system with those requirements. It shall contain, at a minimum, the elements set out in Annex IV.

2. Where a high-risk AI system related to a product, to which the legal acts listed in Annex II, section A apply, is placed on the market or put into service one single technical documentation shall be drawn up containing all the information set out in Annex IV as well as the information required under those legal acts.

3. The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend Annex IV where necessary to ensure that, in the light of technical progress, the technical documentation provides all the necessary information to assess the compliance of the system with the requirements set out in this Chapter.

*Article 12*
*Record-keeping*

1. High-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events ('logs') while the high-risk AI systems is operating. Those logging capabilities shall conform to recognised standards or common specifications.

2. The logging capabilities shall ensure a level of traceability of the AI system's functioning throughout its lifecycle that is appropriate to the intended purpose of the system.

3. In particular, logging capabilities shall enable the monitoring of the operation of the high-risk AI system with respect to the occurrence of situations that may result in the AI system presenting a risk within the meaning of Article 65(1) or lead to a substantial modification, and facilitate the post-market monitoring referred to in Article 61.

4. For high-risk AI systems referred to in paragraph 1, point (a) of Annex III, the logging capabilities shall provide, at a minimum:

   (a) recording of the period of each use of the system (start date and time and end date and time of each use);

   (b) the reference database against which input data has been checked by the system;

   (c) the input data for which the search has led to a match;

   (d) the identification of the natural persons involved in the verification of the results, as referred to in Article 14 (5).

*Article 13*
*Transparency and provision of information to users*

1. High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured, with a view to achieving compliance with the relevant obligations of the user and of the provider set out in Chapter 3 of this Title.

2. High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to users.

3. The information referred to in paragraph 2 shall specify:

   (a) the identity and the contact details of the provider and, where applicable, of its authorised representative;

(b) the characteristics, capabilities and limitations of performance of the high-risk AI system, including:

(i) its intended purpose;

(ii) the level of accuracy, robustness and cybersecurity referred to in Article 15 against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity;

(iii) any known or foreseeable circumstance, related to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights;

(iv) its performance as regards the persons or groups of persons on which the system is intended to be used;

(v) when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the AI system.

(c) the changes to the high-risk AI system and its performance which have been pre-determined by the provider at the moment of the initial conformity assessment, if any;

(d) the human oversight measures referred to in Article 14, including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the users;

(e) the expected lifetime of the high-risk AI system and any necessary maintenance and care measures to ensure the proper functioning of that AI system, including as regards software updates.

*Article 14*
*Human oversight*

1. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use.

2. Human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular when such risks persist notwithstanding the application of other requirements set out in this Chapter.

3. Human oversight shall be ensured through either one or all of the following measures:

(a) identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service;

(b) identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the user.

4. The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances:

(a) fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible;

(b) remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias'), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons;

(c) be able to correctly interpret the high-risk AI system's output, taking into account in particular the characteristics of the system and the interpretation tools and methods available;

(d) be able to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system;

(e) be able to intervene on the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure.

5. For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 shall be such as to ensure that, in addition, no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been verified and confirmed by at least two natural persons.

*Article 15*
*Accuracy, robustness and cybersecurity*

1. High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle.

2. The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use.

3. High-risk AI systems shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems.

The robustness of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans.

High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way to ensure that possibly biased outputs due to outputs used as an input for future operations ('feedback loops') are duly addressed with appropriate mitigation measures.

4. High-risk AI systems shall be resilient as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities.

The technical solutions aimed at ensuring the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks.

The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent and control for attacks trying to manipulate the training dataset ('data poisoning'), inputs designed to cause the model to make a mistake ('adversarial examples'), or model flaws.

## CHAPTER 3

## OBLIGATIONS OF PROVIDERS AND USERS OF HIGH-RISK AI SYSTEMS AND OTHER PARTIES

### *Article 16*
### *Obligations of providers of high-risk AI systems*

Providers of high-risk AI systems shall:

(a) ensure that their high-risk AI systems are compliant with the requirements set out in Chapter 2 of this Title;

(b) have a quality management system in place which complies with Article 17;

(c) draw-up the technical documentation of the high-risk AI system;

(d) when under their control, keep the logs automatically generated by their high-risk AI systems;

(e) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure, prior to its placing on the market or putting into service;

(f) comply with the registration obligations referred to in Article 51;

(g) take the necessary corrective actions, if the high-risk AI system is not in conformity with the requirements set out in Chapter 2 of this Title;

(h) inform the national competent authorities of the Member States in which they made the AI system available or put it into service and, where applicable, the notified body of the non-compliance and of any corrective actions taken;

(i) to affix the CE marking to their high-risk AI systems to indicate the conformity with this Regulation in accordance with Article 49;

(j) upon request of a national competent authority, demonstrate the conformity of the high-risk AI system with the requirements set out in Chapter 2 of this Title.

*Article 17*
*Quality management system*

1. Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:

(a) a strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system;

(b) techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system;

(c) techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system;

(d) examination, test and validation procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out;

(e) technical specifications, including standards, to be applied and, where the relevant harmonised standards are not applied in full, the means to be used to ensure that the high-risk AI system complies with the requirements set out in Chapter 2 of this Title;

(f) systems and procedures for data management, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into service of high-risk AI systems;

(g) the risk management system referred to in Article 9;

(h) the setting-up, implementation and maintenance of a post-market monitoring system, in accordance with Article 61;

(i) procedures related to the reporting of serious incidents and of malfunctioning in accordance with Article 62;

(j) the handling of communication with national competent authorities, competent authorities, including sectoral ones, providing or supporting the access to data, notified bodies, other operators, customers or other interested parties;

(k) systems and procedures for record keeping of all relevant documentation and information;

(l) resource management, including security of supply related measures;

(m) an accountability framework setting out the responsibilities of the management and other staff with regard to all aspects listed in this paragraph.

2. The implementation of aspects referred to in paragraph 1 shall be proportionate to the size of the provider's organisation.

3. For providers that are credit institutions regulated by Directive 2013/36/ EU, the obligation to put a quality management system in place shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive. In that context, any harmonised standards referred to in Article 40 of this Regulation shall be taken into account.

*Article 18*
*Obligation to draw up technical documentation*

1. Providers of high-risk AI systems shall draw up the technical documentation referred to in Article 11 in accordance with Annex IV.

2. Providers that are credit institutions regulated by Directive 2013/36/EU shall maintain the technical documentation as part of the documentation concerning internal governance, arrangements, processes and mechanisms pursuant to Article 74 of that Directive.

*Article 19*
*Conformity assessment*

1. Providers of high-risk AI systems shall ensure that their systems undergo the relevant conformity assessment procedure in accordance with Article 43, prior to their placing on the market or putting into service. Where the compliance of the AI systems with the requirements set out in Chapter 2 of this Title has been demonstrated following that conformity assessment, the providers shall draw up an EU declaration of conformity in accordance with Article 48 and affix the CE marking of conformity in accordance with Article 49.

2. For high-risk AI systems referred to in point 5(b) of Annex III that are placed on the market or put into service by providers that are credit institutions regulated by Directive 2013/36/EU, the conformity assessment shall be carried out as part of the procedure referred to in Articles 97 to101 of that Directive.

*Article 20*
*Automatically generated logs*

1. Providers of high-risk AI systems shall keep the logs automatically generated by their high-risk AI systems, to the extent such logs are under their control by virtue of a contractual arrangement with the user or otherwise by law. The logs shall be kept for a period that is appropriate in the light of the intended purpose of high-risk AI system and applicable legal obligations under Union or national law.

2. Providers that are credit institutions regulated by Directive 2013/36/EU shall maintain the logs automatically generated by their high-risk AI systems as part of the documentation under Articles 74 of that Directive.

*Article 21*
*Corrective actions*

Providers of high-risk AI systems which consider or have reason to consider that a high-risk AI system which they have placed on the market or put into service is not in conformity with this Regulation shall immediately take the necessary corrective actions to bring that system into conformity, to withdraw it or to recall it, as appropriate. They shall inform the distributors of the high-risk AI system in question and, where applicable, the authorised representative and importers accordingly.

*Article 22*
*Duty of information*

Where the high-risk AI system presents a risk within the meaning of Article 65(1) and that risk is known to the provider of the system, that provider shall immediately inform the national competent authorities of the Member States in which it made the system available and, where applicable, the notified body that issued a certificate for the high-risk AI system, in particular of the non-compliance and of any corrective actions taken.

*Article 23*
*Cooperation with competent authorities*

Providers of high-risk AI systems shall, upon request by a national competent authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the high-risk AI system with the requirements set out in Chapter 2 of this Title, in an official Union language determined by the Member State concerned. Upon a reasoned request from a national competent authority, providers shall also give that authority access to the logs automatically generated by the high-risk AI system, to the extent such logs are under their control by virtue of a contractual arrangement with the user or otherwise by law.

*Article 24*
*Obligations of product manufacturers*

Where a high-risk AI system related to products to which the legal acts listed in Annex II, section A, apply, is placed on the market or put into service together with the product manufactured in accordance with those legal acts and under the name of the product manufacturer, the manufacturer of the product shall take the responsibility of the compliance of the AI system with this Regulation and, as far as the AI system is concerned, have the same obligations imposed by the present Regulation on the provider.

*Article 25*
*Authorised representatives*

1. Prior to making their systems available on the Union market, where an importer cannot be identified, providers established outside the Union shall, by written mandate, appoint an authorised representative which is established in the Union.

2. The authorised representative shall perform the tasks specified in the mandate received from the provider. The mandate shall empower the authorised representative to carry out the following tasks:

   (a) keep a copy of the EU declaration of conformity and the technical documentation at the disposal of the national competent authorities and national authorities referred to in Article 63(7);

   (b) provide a national competent authority, upon a reasoned request, with all the information and documentation necessary to demonstrate the conformity of a high-risk AI system with the requirements set out in Chapter 2 of this Title, including access to the logs automatically generated by the high-risk AI system to the extent such logs are under the control of the provider by virtue of a contractual arrangement with the user or otherwise by law;

   (c) cooperate with competent national authorities, upon a reasoned request, on any action the latter takes in relation to the high-risk AI system.

*Article 26*
*Obligations of importers*

1. Before placing a high-risk AI system on the market, importers of such system shall ensure that:

   (a) the appropriate conformity assessment procedure has been carried out by the provider of that AI system

   (b) the provider has drawn up the technical documentation in accordance with Annex IV;

   (c) the system bears the required conformity marking and is accompanied by the required documentation and instructions of use.

2. Where an importer considers or has reason to consider that a high-risk AI system is not in conformity with this Regulation, it shall not place that system on the market until that AI system has been brought into conformity. Where the high-risk AI system presents a risk within the meaning of Article 65(1), the importer shall inform the provider of the AI system and the market surveillance authorities to that effect.

3. Importers shall indicate their name, registered trade name or registered trade mark, and the address at which they can be contacted on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable.

4. Importers shall ensure that, while a high-risk AI system is under their responsibility, where applicable, storage or transport conditions do not jeopardise its compliance with the requirements set out in Chapter 2 of this Title.

5. Importers shall provide national competent authorities, upon a reasoned request, with all necessary information and documentation to demonstrate the conformity of a high-risk AI system with the requirements set out in Chapter 2 of this Title in a language which can be easily understood by that national competent authority, including access to the logs automatically generated by the high-risk AI system to the extent such logs are under the control of the provider by virtue of a contractual arrangement with the user or otherwise by law. They shall also cooperate with those authorities on any action national competent authority takes in relation to that system.

*Article 27*
*Obligations of distributors*

1. Before making a high-risk AI system available on the market, distributors shall verify that the high-risk AI system bears the required CE conformity marking, that it is accompanied by the required documentation and instruction of use, and that the provider and the importer of the system, as applicable, have complied with the obligations set out in this Regulation.

2. Where a distributor considers or has reason to consider that a high-risk AI system is not in conformity with the requirements set out in Chapter 2 of this Title, it shall not make the high-risk AI system available on the market until that system has been brought into conformity with those requirements. Furthermore, where the system presents a risk within the meaning of Article 65(1), the distributor shall inform the provider or the importer of the system, as applicable, to that effect.

3. Distributors shall ensure that, while a high-risk AI system is under their responsibility, where applicable, storage or transport conditions do not jeopardise the compliance of the system with the requirements set out in Chapter 2 of this Title.

4. A distributor that considers or has reason to consider that a high-risk AI system which it has made available on the market is not in conformity with the requirements set out in Chapter 2 of this Title shall take the corrective actions necessary to bring that system into conformity with those requirements, to withdraw it or recall it or shall ensure that the provider, the importer or any relevant operator, as appropriate, takes those corrective actions. Where the high-risk AI system presents a risk within

the meaning of Article 65(1), the distributor shall immediately inform the national competent authorities of the Member States in which it has made the product available to that effect, giving details, in particular, of the non-compliance and of any corrective actions taken.

5. Upon a reasoned request from a national competent authority, distributors of high-risk AI systems shall provide that authority with all the information and documentation necessary to demonstrate the conformity of a high-risk system with the requirements set out in Chapter 2 of this Title. Distributors shall also cooperate with that national competent authority on any action taken by that authority.

*Article 28*
*Obligations of distributors, importers, users or any other third-party*

1. Any distributor, importer, user or other third-party shall be considered a provider for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16, in any of the following circumstances:

   (a) they place on the market or put into service a high-risk AI system under their name or trademark;

   (b) they modify the intended purpose of a high-risk AI system already placed on the market or put into service;

   (c) they make a substantial modification to the high-risk AI system.

2. Where the circumstances referred to in paragraph 1, point (b) or (c), occur, the provider that initially placed the high-risk AI system on the market or put it into service shall no longer be considered a provider for the purposes of this Regulation.

*Article 29*
*Obligations of users of high-risk AI systems*

1. Users of high-risk AI systems shall use such systems in accordance with the instructions of use accompanying the systems, pursuant to paragraphs 2 and 5.

2. The obligations in paragraph 1 are without prejudice to other user obligations under Union or national law and to the user's discretion in organising its own resources and activities for the purpose of implementing the human oversight measures indicated by the provider.

3. Without prejudice to paragraph 1, to the extent the user exercises control over the input data, that user shall ensure that input data is relevant in view of the intended purpose of the high-risk AI system.

4. Users shall monitor the operation of the high-risk AI system on the basis of the instructions of use. When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of Article 65(1) they shall inform the provider or distributor and suspend the use of the system. They shall also inform the provider or distributor when they

have identified any serious incident or any malfunctioning within the meaning of Article 62 and interrupt the use of the AI system. In case the user is not able to reach the provider, Article 62 shall apply mutatis mutandis.

For users that are credit institutions regulated by Directive 2013/36/EU, the monitoring obligation set out in the first subparagraph shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive.

5. Users of high-risk AI systems shall keep the logs automatically generated by that high-risk AI system, to the extent such logs are under their control. The logs shall be kept for a period that is appropriate in the light of the intended purpose of the high-risk AI system and applicable legal obligations under Union or national law.

Users that are credit institutions regulated by Directive 2013/36/EU shall maintain the logs as part of the documentation concerning internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive.

6. Users of high-risk AI systems shall use the information provided under Article 13 to comply with their obligation to carry out a data protection impact assessment under Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, where applicable.

## CHAPTER 4

## NOTIFIYING AUTHORITIES AND NOTIFIED BODIES

### *Article 30*
### *Notifying authorities*

1. Each Member State shall designate or establish a notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring.

2. Member States may designate a national accreditation body referred to in Regulation (EC) No 765/2008 as a notifying authority.

3. Notifying authorities shall be established, organised and operated in such a way that no conflict of interest arises with conformity assessment bodies and the objectivity and impartiality of their activities are safeguarded.

4. Notifying authorities shall be organised in such a way that decisions relating to the notification of conformity assessment bodies are taken by competent persons different from those who carried out the assessment of those bodies.

5. Notifying authorities shall not offer or provide any activities that conformity assessment bodies perform or any consultancy services on a commercial or competitive basis.

6. Notifying authorities shall safeguard the confidentiality of the information they obtain.

7. Notifying authorities shall have a sufficient number of competent personnel at their disposal for the proper performance of their tasks.

8. Notifying authorities shall make sure that conformity assessments are carried out in a proportionate manner, avoiding unnecessary burdens for providers and that notified bodies perform their activities taking due account of the size of an undertaking, the sector in which it operates, its structure and the degree of complexity of the AI system in question.

*Article 31*
*Application of a conformity assessment body for notification*

1. Conformity assessment bodies shall submit an application for notification to the notifying authority of the Member State in which they are established.

2. The application for notification shall be accompanied by a description of the conformity assessment activities, the conformity assessment module or modules and the artificial intelligence technologies for which the conformity assessment body claims to be competent, as well as by an accreditation certificate, where one exists, issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 33. Any valid document related to existing designations of the applicant notified body under any other Union harmonisation legislation shall be added.

3. Where the conformity assessment body concerned cannot provide an accreditation certificate, it shall provide the notifying authority with the documentary evidence necessary for the verification, recognition and regular monitoring of its compliance with the requirements laid down in Article 33. For notified bodies which are designated under any other Union harmonisation legislation, all documents and certificates linked to those designations may be used to support their designation procedure under this Regulation, as appropriate.

*Article 32*
*Notification procedure*

1. Notifying authorities may notify only conformity assessment bodies which have satisfied the requirements laid down in Article 33.

2. Notifying authorities shall notify the Commission and the other Member States using the electronic notification tool developed and managed by the Commission.

3. The notification shall include full details of the conformity assessment activities, the conformity assessment module or modules and the artificial intelligence technologies concerned.

4. The conformity assessment body concerned may perform the activities of a notified body only where no objections are raised by the Commission or the other Member States within one month of a notification.

5. Notifying authorities shall notify the Commission and the other Member States of any subsequent relevant changes to the notification.

*Article 33*
*Notified bodies*

1. Notified bodies shall verify the conformity of high-risk AI system in accordance with the conformity assessment procedures referred to in Article 43.

2. Notified bodies shall satisfy the organisational, quality management, resources and process requirements that are necessary to fulfil their tasks.

3. The organisational structure, allocation of responsibilities, reporting lines and operation of notified bodies shall be such as to ensure that there is confidence in the performance by and in the results of the conformity assessment activities that the notified bodies conduct.

4. Notified bodies shall be independent of the provider of a high-risk AI system in relation to which it performs conformity assessment activities. Notified bodies shall also be independent of any other operator having an economic interest in the high-risk AI system that is assessed, as well as of any competitors of the provider.

5. Notified bodies shall be organised and operated so as to safeguard the independence, objectivity and impartiality of their activities. Notified bodies shall document and implement a structure and procedures to safeguard impartiality and to promote and apply the principles of impartiality throughout their organisation, personnel and assessment activities.

6. Notified bodies shall have documented procedures in place ensuring that their personnel, committees, subsidiaries, subcontractors and any associated body or personnel of external bodies respect the confidentiality of the information which comes into their possession during the performance of conformity assessment activities, except when disclosure is required by law. The staff of notified bodies shall be bound to observe professional secrecy with regard to all information obtained in carrying out their tasks under this Regulation, except in relation to the notifying authorities of the Member State in which their activities are carried out.

7. Notified bodies shall have procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the AI system in question.

8. Notified bodies shall take out appropriate liability insurance for their conformity assessment activities, unless liability is assumed by the Member State concerned in accordance with national law or that Member State is directly responsible for the conformity assessment.

9. Notified bodies shall be capable of carrying out all the tasks falling to them under this Regulation with the highest degree of professional integrity and the requisite competence in the specific field, whether those tasks are carried out by notified bodies themselves or on their behalf and under their responsibility.

10. Notified bodies shall have sufficient internal competences to be able to effectively evaluate the tasks conducted by external parties on their behalf. To that end, at all times and for each conformity assessment procedure and each type of high-risk AI system in relation to which they have been designated, the notified body shall have permanent availability of sufficient administrative, technical and scientific personnel who possess experience and knowledge relating to the relevant artificial intelligence technologies, data and data computing and to the requirements set out in Chapter 2 of this Title.

11. Notified bodies shall participate in coordination activities as referred to in Article 38. They shall also take part directly or be represented in European standardisation organisations, or ensure that they are aware and up to date in respect of relevant standards.

12. Notified bodies shall make available and submit upon request all relevant documentation, including the providers' documentation, to the notifying authority referred to in Article 30 to allow it to conduct its assessment, designation, notification, monitoring and surveillance activities and to facilitate the assessment outlined in this Chapter.

*Article 34*
*Subsidiaries of and subcontracting by notified bodies*

1. Where a notified body subcontracts specific tasks connected with the conformity assessment or has recourse to a subsidiary, it shall ensure that the subcontractor or the subsidiary meets the requirements laid down in Article 33 and shall inform the notifying authority accordingly.

2. Notified bodies shall take full responsibility for the tasks performed by subcontractors or subsidiaries wherever these are established.

3. Activities may be subcontracted or carried out by a subsidiary only with the agreement of the provider.

4. Notified bodies shall keep at the disposal of the notifying authority the relevant documents concerning the assessment of the qualifications of the subcontractor or the subsidiary and the work carried out by them under this Regulation.

*Article 35*
*Identification numbers and lists of notified bodies designated under this Regulation*

1. The Commission shall assign an identification number to notified bodies. It shall assign a single number, even where a body is notified under several Union acts.

2. The Commission shall make publicly available the list of the bodies notified under this Regulation, including the identification numbers that have been assigned to them and the activities for which they have been notified. The Commission shall ensure that the list is kept up to date.

*Article 36*
*Changes to notifications*

1. Where a notifying authority has suspicions or has been informed that a notified body no longer meets the requirements laid down in Article 33, or that it is failing to fulfil its obligations, that authority shall without delay investigate the matter with the utmost diligence. In that context, it shall inform the notified body concerned about the objections raised and give it the possibility to make its views known. If the notifying authority comes to the conclusion that the notified body investigation no longer meets the requirements laid down in Article 33 or that it is failing to fulfil its obligations, it shall restrict, suspend or withdraw the notification as appropriate, depending on the seriousness of the failure. It shall also immediately inform the Commission and the other Member States accordingly.

2. In the event of restriction, suspension or withdrawal of notification, or where the notified body has ceased its activity, the notifying authority shall take appropriate steps to ensure that the files of that notified body are either taken over by another notified body or kept available for the responsible notifying authorities at their request.

*Article 37*
*Challenge to the competence of notified bodies*

1. The Commission shall, where necessary, investigate all cases where there are reasons to doubt whether a notified body complies with the requirements laid down in Article 33.

2. The Notifying authority shall provide the Commission, on request, with all relevant information relating to the notification of the notified body concerned.

3. The Commission shall ensure that all confidential information obtained in the course of its investigations pursuant to this Article is treated confidentially.

4. Where the Commission ascertains that a notified body does not meet or no longer meets the requirements laid down in Article 33, it shall adopt a reasoned decision requesting the notifying Member State to take the necessary corrective measures, including withdrawal of notification if necessary. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 74(2).

*Article 38*
*Coordination of notified bodies*

1. The Commission shall ensure that, with regard to the areas covered by this Regulation, appropriate coordination and cooperation between notified bodies active

in the conformity assessment procedures of AI systems pursuant to this Regulation are put in place and properly operated in the form of a sectoral group of notified bodies**.**

2. Member States shall ensure that the bodies notified by them participate in the work of that group, directly or by means of designated representatives.

*Article 39*
*Conformity assessment bodies of third countries*

Conformity assessment bodies established under the law of a third country with which the Union has concluded an agreement may be authorised to carry out the activities of notified Bodies under this Regulation.

## CHAPTER 5

## STANDARDS, CONFORMITY ASSESSMENT, CERTIFICATES, REGISTRATION

*Article 40*
*Harmonised standards*

High-risk AI systems which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title, to the extent those standards cover those requirements.

*Article 41*
*Common specifications*

1. Where harmonised standards referred to in Article 40 do not exist or where the Commission considers that the relevant harmonised standards are insufficient or that there is a need to address specific safety or fundamental right concerns, the Commission may, by means of implementing acts, adopt common specifications in respect of the requirements set out in Chapter 2 of this Title. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2).

2. The Commission, when preparing the common specifications referred to in paragraph 1, shall gather the views of relevant bodies or expert groups established under relevant sectorial Union law.

3. High-risk AI systems which are in conformity with the common specifications referred to in paragraph 1 shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title, to the extent those common specifications cover those requirements.

4. Where providers do not comply with the common specifications referred to in paragraph 1, they shall duly justify that they have adopted technical solutions that are at least equivalent thereto.

*Article 42*
*Presumption of conformity with certain requirements*

1. Taking into account their intended purpose, high-risk AI systems that have been trained and tested on data concerning the specific geographical, behavioural and functional setting within which they are intended to be used shall be presumed to be in compliance with the requirement set out in Article 10(4).

2. High-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council[63] and the references of which have been published in the Official Journal of the European Union shall be presumed to be in compliance with the cybersecurity requirements set out in Article 15 of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements.

*Article 43*
*Conformity assessment*

1. For high-risk AI systems listed in point 1 of Annex III, where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has applied harmonised standards referred to in Article 40, or, where applicable, common specifications referred to in Article 41, the provider shall follow one of the following procedures:

   (a) the conformity assessment procedure based on internal control referred to in Annex VI;

   (b) the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation, with the involvement of a notified body, referred to in Annex VII.

   Where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has not applied or has applied only in part harmonised standards referred to in Article 40, or where such harmonised standards do not exist and common specifications referred to in Article 41 are not available, the provider shall follow the conformity assessment procedure set out in Annex VII.

   For the purpose of the conformity assessment procedure referred to in Annex VII, the provider may choose any of the notified bodies. However, when the system is

[63] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 1).

intended to be put into service by law enforcement, immigration or asylum authorities as well as EU institutions, bodies or agencies, the market surveillance authority referred to in Article 63(5) or (6), as applicable, shall act as a notified body.

2. For high-risk AI systems referred to in points 2 to 8 of Annex III, providers shall follow the conformity assessment procedure based on internal control as referred to in Annex VI, which does not provide for the involvement of a notified body. For high-risk AI systems referred to in point 5(b) of Annex III, placed on the market or put into service by credit institutions regulated by Directive 2013/36/EU, the conformity assessment shall be carried out as part of the procedure referred to in Articles 97 to101 of that Directive.

3. For high-risk AI systems, to which legal acts listed in Annex II, section A, apply, the provider shall follow the relevant conformity assessment as required under those legal acts. The requirements set out in Chapter 2 of this Title shall apply to those high-risk AI systems and shall be part of that assessment. Points 4.3., 4.4., 4.5. and the fifth paragraph of point 4.6 of Annex VII shall also apply.

   For the purpose of that assessment, notified bodies which have been notified under those legal acts shall be entitled to control the conformity of the high-risk AI systems with the requirements set out in Chapter 2 of this Title, provided that the compliance of those notified bodies with requirements laid down in Article 33(4), (9) and (10) has been assessed in the context of the notification procedure under those legal acts.

   Where the legal acts listed in Annex II, section A, enable the manufacturer of the product to opt out from a third-party conformity assessment, provided that that manufacturer has applied all harmonised standards covering all the relevant requirements, that manufacturer may make use of that option only if he has also applied harmonised standards or, where applicable, common specifications referred to in Article 41, covering the requirements set out in Chapter 2 of this Title.

4. High-risk AI systems shall undergo a new conformity assessment procedure whenever they are substantially modified, regardless of whether the modified system is intended to be further distributed or continues to be used by the current user.

   For high-risk AI systems that continue to learn after being placed on the market or put into service, changes to the high-risk AI system and its performance that have been pre-determined by the provider at the moment of the initial conformity assessment and are part of the information contained in the technical documentation referred to in point 2(f) of Annex IV, shall not constitute a substantial modification.

5. The Commission is empowered to adopt delegated acts in accordance with Article 73 for the purpose of updating Annexes VI and Annex VII in order to introduce elements of the conformity assessment procedures that become necessary in light of technical progress.

6. The Commission is empowered to adopt delegated acts to amend paragraphs 1 and 2 in order to subject high-risk AI systems referred to in points 2 to 8 of Annex III to the conformity assessment procedure referred to in Annex VII or parts thereof. The Commission shall adopt such delegated acts taking into account the effectiveness of the conformity assessment procedure based on internal control referred to in Annex VI in preventing or minimizing the risks to health and safety and protection of

fundamental rights posed by such systems as well as the availability of adequate capacities and resources among notified bodies.

*Article 44*
*Certificates*

1. Certificates issued by notified bodies in accordance with Annex VII shall be drawn-up in an official Union language determined by the Member State in which the notified body is established or in an official Union language otherwise acceptable to the notified body.

2. Certificates shall be valid for the period they indicate, which shall not exceed five years. On application by the provider, the validity of a certificate may be extended for further periods, each not exceeding five years, based on a re-assessment in accordance with the applicable conformity assessment procedures.

3. Where a notified body finds that an AI system no longer meets the requirements set out in Chapter 2 of this Title, it shall, taking account of the principle of proportionality, suspend or withdraw the certificate issued or impose any restrictions on it, unless compliance with those requirements is ensured by appropriate corrective action taken by the provider of the system within an appropriate deadline set by the notified body. The notified body shall give reasons for its decision.

*Article 45*
*Appeal against decisions of notified bodies*

Member States shall ensure that an appeal procedure against decisions of the notified bodies is available to parties having a legitimate interest in that decision.

*Article 46*
*Information obligations of notified bodies*

1. Notified bodies shall inform the notifying authority of the following:

   (a) any Union technical documentation assessment certificates, any supplements to those certificates, quality management system approvals issued in accordance with the requirements of Annex VII;

   (b) any refusal, restriction, suspension or withdrawal of a Union technical documentation assessment certificate or a quality management system approval issued in accordance with the requirements of Annex VII;

   (c) any circumstances affecting the scope of or conditions for notification;

   (d) any request for information which they have received from market surveillance authorities regarding conformity assessment activities;

   (e) on request, conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.

2. Each notified body shall inform the other notified bodies of:

(a) quality management system approvals which it has refused, suspended or withdrawn, and, upon request, of quality system approvals which it has issued;

(b) EU technical documentation assessment certificates or any supplements thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, of the certificates and/or supplements thereto which it has issued.

3. Each notified body shall provide the other notified bodies carrying out similar conformity assessment activities covering the same artificial intelligence technologies with relevant information on issues relating to negative and, on request, positive conformity assessment results.

*Article 47*
*Derogation from conformity assessment procedure*

1. By way of derogation from Article 43, any market surveillance authority may authorise the placing on the market or putting into service of specific high-risk AI systems within the territory of the Member State concerned, for exceptional reasons of public security or the protection of life and health of persons, environmental protection and the protection of key industrial and infrastructural assets. That authorisation shall be for a limited period of time, while the necessary conformity assessment procedures are being carried out, and shall terminate once those procedures have been completed. The completion of those procedures shall be undertaken without undue delay.

2. The authorisation referred to in paragraph 1 shall be issued only if the market surveillance authority concludes that the high-risk AI system complies with the requirements of Chapter 2 of this Title. The market surveillance authority shall inform the Commission and the other Member States of any authorisation issued pursuant to paragraph 1.

3. Where, within 15 calendar days of receipt of the information referred to in paragraph 2, no objection has been raised by either a Member State or the Commission in respect of an authorisation issued by a market surveillance authority of a Member State in accordance with paragraph 1, that authorisation shall be deemed justified.

4. Where, within 15 calendar days of receipt of the notification referred to in paragraph 2, objections are raised by a Member State against an authorisation issued by a market surveillance authority of another Member State, or where the Commission considers the authorisation to be contrary to Union law or the conclusion of the Member States regarding the compliance of the system as referred to in paragraph 2 to be unfounded, the Commission shall without delay enter into consultation with the relevant Member State; the operator(s) concerned shall be consulted and have the possibility to present their views. In view thereof, the Commission shall decide whether the authorisation is justified or not. The Commission shall address its decision to the Member State concerned and the relevant operator or operators.

5. If the authorisation is considered unjustified, this shall be withdrawn by the market surveillance authority of the Member State concerned.

6. By way of derogation from paragraphs 1 to 5, for high-risk AI systems intended to be used as safety components of devices, or which are themselves devices, covered by Regulation (EU) 2017/745 and Regulation (EU) 2017/746, Article 59 of Regulation (EU) 2017/745 and Article 54 of Regulation (EU) 2017/746 shall apply also with regard to the derogation from the conformity assessment of the compliance with the requirements set out in Chapter 2 of this Title.

*Article 48*
*EU declaration of conformity*

1. The provider shall draw up a written EU declaration of conformity for each AI system and keep it at the disposal of the national competent authorities for 10 years after the AI system has been placed on the market or put into service. The EU declaration of conformity shall identify the AI system for which it has been drawn up. A copy of the EU declaration of conformity shall be given to the relevant national competent authorities upon request.

2. The EU declaration of conformity shall state that the high-risk AI system in question meets the requirements set out in Chapter 2 of this Title. The EU declaration of conformity shall contain the information set out in Annex V and shall be translated into an official Union language or languages required by the Member State(s) in which the high-risk AI system is made available.

3. Where high-risk AI systems are subject to other Union harmonisation legislation which also requires an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all Union legislations applicable to the high-risk AI system. The declaration shall contain all the information required for identification of the Union harmonisation legislation to which the declaration relates.

4. By drawing up the EU declaration of conformity, the provider shall assume responsibility for compliance with the requirements set out in Chapter 2 of this Title. The provider shall keep the EU declaration of conformity up-to-date as appropriate.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 73 for the purpose of updating the content of the EU declaration of conformity set out in Annex V in order to introduce elements that become necessary in light of technical progress.

*Article 49*
*CE marking of conformity*

1. The CE marking shall be affixed visibly, legibly and indelibly for high-risk AI systems. Where that is not possible or not warranted on account of the nature of the high-risk AI system, it shall be affixed to the packaging or to the accompanying documentation, as appropriate.

2. The CE marking referred to in paragraph 1 of this Article shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.

3. Where applicable, the CE marking shall be followed by the identification number of the notified body responsible for the conformity assessment procedures set out in Article 43. The identification number shall also be indicated in any promotional material which mentions that the high-risk AI system fulfils the requirements for CE marking.

*Article 50*
*Document retention*

The provider shall, for a period ending 10 years after the AI system has been placed on the market or put into service, keep at the disposal of the national competent authorities:

(a) the technical documentation referred to in Article 11;

(b) the documentation concerning the quality management system referred to Article 17;

(c) the documentation concerning the changes approved by notified bodies where applicable;

(d) the decisions and other documents issued by the notified bodies where applicable;

(e) the EU declaration of conformity referred to in Article 48.

*Article 51*
*Registration*

Before placing on the market or putting into service a high-risk AI system referred to in Article 6(2), the provider or, where applicable, the authorised representative shall register that system in the EU database referred to in Article 60.

# TITLE IV

# TRANSPARENCY OBLIGATIONS FOR CERTAIN AI SYSTEMS

*Article 52*
*Transparency obligations for certain AI systems*

1. Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence.

2. Users of an emotion recognition system or a biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto. This obligation shall not apply to AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences.

3. Users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake'), shall disclose that the content has been artificially generated or manipulated.

However, the first subparagraph shall not apply where the use is authorised by law to detect, prevent, investigate and prosecute criminal offences or it is necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Fundamental Rights of the EU, and subject to appropriate safeguards for the rights and freedoms of third parties.

4. Paragraphs 1, 2 and 3 shall not affect the requirements and obligations set out in Title III of this Regulation.

**TITLE V**

# MEASURES IN SUPPORT OF INNOVATION

*Article 53*
*AI regulatory sandboxes*

1. AI regulatory sandboxes established by one or more Member States competent authorities or the European Data Protection Supervisor shall provide a controlled environment that facilitates the development, testing and validation of innovative AI systems for a limited time before their placement on the market or putting into service pursuant to a specific plan. This shall take place under the direct supervision and guidance by the competent authorities with a view to ensuring compliance with the requirements of this Regulation and, where relevant, other Union and Member States legislation supervised within the sandbox.

2. Member States shall ensure that to the extent the innovative AI systems involve the processing of personal data or otherwise fall under the supervisory remit of other national authorities or competent authorities providing or supporting access to data, the national data protection authorities and those other national authorities are associated to the operation of the AI regulatory sandbox.

3. The AI regulatory sandboxes shall not affect the supervisory and corrective powers of the competent authorities. Any significant risks to health and safety and fundamental rights identified during the development and testing of such systems shall result in immediate mitigation and, failing that, in the suspension of the development and testing process until such mitigation takes place.

4. Participants in the AI regulatory sandbox shall remain liable under applicable Union and Member States liability legislation for any harm inflicted on third parties as a result from the experimentation taking place in the sandbox.

5. Member States' competent authorities that have established AI regulatory sandboxes shall coordinate their activities and cooperate within the framework of the European Artificial Intelligence Board. They shall submit annual reports to the Board and the

Commission on the results from the implementation of those scheme, including good practices, lessons learnt and recommendations on their setup and, where relevant, on the application of this Regulation and other Union legislation supervised within the sandbox.

6. The modalities and the conditions of the operation of the AI regulatory sandboxes, including the eligibility criteria and the procedure for the application, selection, participation and exiting from the sandbox, and the rights and obligations of the participants shall be set out in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2).

*Article 54*
*Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox*

1. In the AI regulatory sandbox personal data lawfully collected for other purposes shall be processed for the purposes of developing and testing certain innovative AI systems in the sandbox under the following conditions:

   (a) the innovative AI systems shall be developed for safeguarding substantial public interest in one or more of the following areas:

      (i) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, under the control and responsibility of the competent authorities. The processing shall be based on Member State or Union law;

      (ii) public safety and public health, including disease prevention, control and treatment;

      (iii) a high level of protection and improvement of the quality of the environment;

   (b) the data processed are necessary for complying with one or more of the requirements referred to in Title III, Chapter 2 where those requirements cannot be effectively fulfilled by processing anonymised, synthetic or other non-personal data;

   (c) there are effective monitoring mechanisms to identify if any high risks to the fundamental rights of the data subjects may arise during the sandbox experimentation as well as response mechanism to promptly mitigate those risks and, where necessary, stop the processing;

   (d) any personal data to be processed in the context of the sandbox are in a functionally separate, isolated and protected data processing environment under the control of the participants and only authorised persons have access to that data;

   (e) any personal data processed are not be transmitted, transferred or otherwise accessed by other parties;

(f) any processing of personal data in the context of the sandbox do not lead to measures or decisions affecting the data subjects;

(g) any personal data processed in the context of the sandbox are deleted once the participation in the sandbox has terminated or the personal data has reached the end of its retention period;

(h) the logs of the processing of personal data in the context of the sandbox are kept for the duration of the participation in the sandbox and 1 year after its termination, solely for the purpose of and only as long as necessary for fulfilling accountability and documentation obligations under this Article or other application Union or Member States legislation;

(i) complete and detailed description of the process and rationale behind the training, testing and validation of the AI system is kept together with the testing results as part of the technical documentation in Annex IV;

(j) a short summary of the AI project developed in the sandbox, its objectives and expected results published on the website of the competent authorities.

2. Paragraph 1 is without prejudice to Union or Member States legislation excluding processing for other purposes than those explicitly mentioned in that legislation.

*Article 55*
*Measures for small-scale providers and users*

1. Member States shall undertake the following actions:

(a) provide small-scale providers and start-ups with priority access to the AI regulatory sandboxes to the extent that they fulfil the eligibility conditions;

(b) organise specific awareness raising activities about the application of this Regulation tailored to the needs of the small-scale providers and users;

(c) where appropriate, establish a dedicated channel for communication with small-scale providers and user and other innovators to provide guidance and respond to queries about the implementation of this Regulation.

2. The specific interests and needs of the small-scale providers shall be taken into account when setting the fees for conformity assessment under Article 43, reducing those fees proportionately to their size and market size.

# TITLE VI

# GOVERNANCE

## CHAPTER 1

## EUROPEAN ARTIFICIAL INTELLIGENCE BOARD

*Article 56*
*Establishment of the European Artificial Intelligence Board*

1. A 'European Artificial Intelligence Board' (the 'Board') is established.

2. The Board shall provide advice and assistance to the Commission in order to:

   (a) contribute to the effective cooperation of the national supervisory authorities and the Commission with regard to matters covered by this Regulation;

   (b) coordinate and contribute to guidance and analysis by the Commission and the national supervisory authorities and other competent authorities on emerging issues across the internal market with regard to matters covered by this Regulation;

   (c) assist the national supervisory authorities and the Commission in ensuring the consistent application of this Regulation.

*Article 57*
*Structure of the Board*

1. The Board shall be composed of the national supervisory authorities, who shall be represented by the head or equivalent high-level official of that authority, and the European Data Protection Supervisor. Other national authorities may be invited to the meetings, where the issues discussed are of relevance for them.

2. The Board shall adopt its rules of procedure by a simple majority of its members, following the consent of the Commission. The rules of procedure shall also contain the operational aspects related to the execution of the Board's tasks as listed in Article 58. The Board may establish sub-groups as appropriate for the purpose of examining specific questions.

3. The Board shall be chaired by the Commission. The Commission shall convene the meetings and prepare the agenda in accordance with the tasks of the Board pursuant to this Regulation and with its rules of procedure. The Commission shall provide administrative and analytical support for the activities of the Board pursuant to this Regulation.

4. The Board may invite external experts and observers to attend its meetings and may hold exchanges with interested third parties to inform its activities to an appropriate extent. To that end the Commission may facilitate exchanges between the Board and other Union bodies, offices, agencies and advisory groups.

*Article 58*
*Tasks of the Board*

When providing advice and assistance to the Commission in the context of Article 56(2), the Board shall in particular:

(a) collect and share expertise and best practices among Member States;

(b) contribute to uniform administrative practices in the Member States, including for the functioning of regulatory sandboxes referred to in Article 53;

(c) issue opinions, recommendations or written contributions on matters related to the implementation of this Regulation, in particular

(i) on technical specifications or existing standards regarding the requirements set out in Title III, Chapter 2,

(ii) on the use of harmonised standards or common specifications referred to in Articles 40 and 41,

(iii) on the preparation of guidance documents, including the guidelines concerning the setting of administrative fines referred to in Article 71.

## CHAPTER 2

### NATIONAL COMPETENT AUTHORITIES

*Article 59*
*Designation of national competent authorities*

1. National competent authorities shall be established or designated by each Member State for the purpose of ensuring the application and implementation of this Regulation. National competent authorities shall be organised so as to safeguard the objectivity and impartiality of their activities and tasks.

2. Each Member State shall designate a national supervisory authority among the national competent authorities. The national supervisory authority shall act as notifying authority and market surveillance authority unless a Member State has organisational and administrative reasons to designate more than one authority.

3. Member States shall inform the Commission of their designation or designations and, where applicable, the reasons for designating more than one authority.

4. Member States shall ensure that national competent authorities are provided with adequate financial and human resources to fulfil their tasks under this Regulation. In particular, national competent authorities shall have a sufficient number of personnel permanently available whose competences and expertise shall include an in-depth understanding of artificial intelligence technologies, data and data computing, fundamental rights, health and safety risks and knowledge of existing standards and legal requirements.

5. Member States shall report to the Commission on an annual basis on the status of the financial and human resources of the national competent authorities with an assessment of their adequacy. The Commission shall transmit that information to the Board for discussion and possible recommendations.

6. The Commission shall facilitate the exchange of experience between national competent authorities.

7. National competent authorities may provide guidance and advice on the implementation of this Regulation, including to small-scale providers. Whenever national competent authorities intend to provide guidance and advice with regard to an AI system in areas covered by other Union legislation, the competent national authorities under that Union legislation shall be consulted, as appropriate. Member States may also establish one central contact point for communication with operators.

8. When Union institutions, agencies and bodies fall within the scope of this Regulation, the European Data Protection Supervisor shall act as the competent authority for their supervision.

**TITLE VII**

# EU DATABASE FOR STAND-ALONE HIGH-RISK AI SYSTEMS

*Article 60*
*EU database for stand-alone high-risk AI systems*

1. The Commission shall, in collaboration with the Member States, set up and maintain a EU database containing information referred to in paragraph 2 concerning high-risk AI systems referred to in Article 6(2) which are registered in accordance with Article 51.

2. The data listed in Annex VIII shall be entered into the EU database by the providers. The Commission shall provide them with technical and administrative support.

3. Information contained in the EU database shall be accessible to the public.

4. The EU database shall contain personal data only insofar as necessary for collecting and processing information in accordance with this Regulation. That information shall include the names and contact details of natural persons who are responsible for registering the system and have the legal authority to represent the provider.

5. The Commission shall be the controller of the EU database. It shall also ensure to providers adequate technical and administrative support.

# TITLE VIII

# POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE

## CHAPTER 1

## POST-MARKET MONITORING

*Article 61*
*Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems*

1. Providers shall establish and document a post-market monitoring system in a manner that is proportionate to the nature of the artificial intelligence technologies and the risks of the high-risk AI system.

2. The post-market monitoring system shall actively and systematically collect, document and analyse relevant data provided by users or collected through other sources on the performance of high-risk AI systems throughout their lifetime, and allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Title III, Chapter 2.

3. The post-market monitoring system shall be based on a post-market monitoring plan. The post-market monitoring plan shall be part of the technical documentation referred to in Annex IV. The Commission shall adopt an implementing act laying down detailed provisions establishing a template for the post-market monitoring plan and the list of elements to be included in the plan.

4. For high-risk AI systems covered by the legal acts referred to in Annex II, where a post-market monitoring system and plan is already established under that legislation, the elements described in paragraphs 1, 2 and 3 shall be integrated into that system and plan as appropriate.

   The first subparagraph shall also apply to high-risk AI systems referred to in point 5(b) of Annex III placed on the market or put into service by credit institutions regulated by Directive 2013/36/EU.

## CHAPTER 2

## SHARING OF INFORMATION ON INCIDENTS AND MALFUNCTIONING

*Article 62*
*Reporting of serious incidents and of malfunctioning*

1. Providers of high-risk AI systems placed on the Union market shall report any serious incident or any malfunctioning of those systems which constitutes a breach of obligations under Union law intended to protect fundamental rights to the market surveillance authorities of the Member States where that incident or breach occurred.

   Such notification shall be made immediately after the provider has established a causal link between the AI system and the incident or malfunctioning or the reasonable likelihood of such a link, and, in any event, not later than 15 days after the providers becomes aware of the serious incident or of the malfunctioning.

2. Upon receiving a notification related to a breach of obligations under Union law intended to protect fundamental rights, the market surveillance authority shall inform the national public authorities or bodies referred to in Article 64(3). The Commission shall develop dedicated guidance to facilitate compliance with the obligations set out in paragraph 1. That guidance shall be issued 12 months after the entry into force of this Regulation, at the latest.

3. For high-risk AI systems referred to in point 5(b) of Annex III which are placed on the market or put into service by providers that are credit institutions regulated by Directive 2013/36/EU and for high-risk AI systems which are safety components of devices, or are themselves devices, covered by Regulation (EU) 2017/745 and Regulation (EU) 2017/746, the notification of serious incidents or malfunctioning shall be limited to those that that constitute a breach of obligations under Union law intended to protect fundamental rights.

## CHAPTER 3

## ENFORCEMENT

*Article 63*
*Market surveillance and control of AI systems in the Union market*

1. Regulation (EU) 2019/1020 shall apply to AI systems covered by this Regulation. However, for the purpose of the effective enforcement of this Regulation:

   (a) any reference to an economic operator under Regulation (EU) 2019/1020 shall be understood as including all operators identified in Title III, Chapter 3 of this Regulation;

(b) any reference to a product under Regulation (EU) 2019/1020 shall be understood as including all AI systems falling within the scope of this Regulation.

2. The national supervisory authority shall report to the Commission on a regular basis the outcomes of relevant market surveillance activities. The national supervisory authority shall report, without delay, to the Commission and relevant national competition authorities any information identified in the course of market surveillance activities that may be of potential interest for the application of Union law on competition rules.

3. For high-risk AI systems, related to products to which legal acts listed in Annex II, section A apply, the market surveillance authority for the purposes of this Regulation shall be the authority responsible for market surveillance activities designated under those legal acts.

4. For AI systems placed on the market, put into service or used by financial institutions regulated by Union legislation on financial services, the market surveillance authority for the purposes of this Regulation shall be the relevant authority responsible for the financial supervision of those institutions under that legislation.

5. For AI systems listed in point 1(a) in so far as the systems are used for law enforcement purposes, points 6 and 7 of Annex III, Member States shall designate as market surveillance authorities for the purposes of this Regulation either the competent data protection supervisory authorities under Directive (EU) 2016/680, or Regulation 2016/679 or the national competent authorities supervising the activities of the law enforcement, immigration or asylum authorities putting into service or using those systems.

6. Where Union institutions, agencies and bodies fall within the scope of this Regulation, the European Data Protection Supervisor shall act as their market surveillance authority.

7. Member States shall facilitate the coordination between market surveillance authorities designated under this Regulation and other relevant national authorities or bodies which supervise the application of Union harmonisation legislation listed in Annex II or other Union legislation that might be relevant for the high-risk AI systems referred to in Annex III.

*Article 64*
*Access to data and documentation*

1. Access to data and documentation in the context of their activities, the market surveillance authorities shall be granted full access to the training, validation and testing datasets used by the provider, including through application programming interfaces ('API') or other appropriate technical means and tools enabling remote access.

2. Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2 and upon a reasoned request, the market surveillance authorities shall be granted access to the source code of the AI system.

3. National public authorities or bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights in relation to the use of high-risk AI systems referred to in Annex III shall have the power to request and access any documentation created or maintained under this Regulation when access to that documentation is necessary for the fulfilment of the competences under their mandate within the limits of their jurisdiction. The relevant public authority or body shall inform the market surveillance authority of the Member State concerned of any such request.

4. By 3 months after the entering into force of this Regulation, each Member State shall identify the public authorities or bodies referred to in paragraph 3 and make a list publicly available on the website of the national supervisory authority. Member States shall notify the list to the Commission and all other Member States and keep the list up to date.

5. Where the documentation referred to in paragraph 3 is insufficient to ascertain whether a breach of obligations under Union law intended to protect fundamental rights has occurred, the public authority or body referred to paragraph 3 may make a reasoned request to the market surveillance authority to organise testing of the high-risk AI system through technical means. The market surveillance authority shall organise the testing with the close involvement of the requesting public authority or body within reasonable time following the request.

6. Any information and documentation obtained by the national public authorities or bodies referred to in paragraph 3 pursuant to the provisions of this Article shall be treated in compliance with the confidentiality obligations set out in Article 70.

*Article 65*
*Procedure for dealing with AI systems presenting a risk at national level*

1. AI systems presenting a risk shall be understood as a product presenting a risk defined in Article 3, point 19 of Regulation (EU) 2019/1020 insofar as risks to the health or safety or to the protection of fundamental rights of persons are concerned.

2. Where the market surveillance authority of a Member State has sufficient reasons to consider that an AI system presents a risk as referred to in paragraph 1, they shall carry out an evaluation of the AI system concerned in respect of its compliance with all the requirements and obligations laid down in this Regulation. When risks to the protection of fundamental rights are present, the market surveillance authority shall also inform the relevant national public authorities or bodies referred to in Article 64(3). The relevant operators shall cooperate as necessary with the market surveillance authorities and the other national public authorities or bodies referred to in Article 64(3).

Where, in the course of that evaluation, the market surveillance authority finds that the AI system does not comply with the requirements and obligations laid down in this Regulation, it shall without delay require the relevant operator to take all appropriate corrective actions to bring the AI system into compliance, to withdraw the AI system from the market, or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe.

The market surveillance authority shall inform the relevant notified body accordingly. Article 18 of Regulation (EU) 2019/1020 shall apply to the measures referred to in the second subparagraph.

3. Where the market surveillance authority considers that non-compliance is not restricted to its national territory, it shall inform the Commission and the other Member States of the results of the evaluation and of the actions which it has required the operator to take.

4. The operator shall ensure that all appropriate corrective action is taken in respect of all the AI systems concerned that it has made available on the market throughout the Union.

5. Where the operator of an AI system does not take adequate corrective action within the period referred to in paragraph 2, the market surveillance authority shall take all appropriate provisional measures to prohibit or restrict the AI system's being made available on its national market, to withdraw the product from that market or to recall it. That authority shall inform the Commission and the other Member States, without delay, of those measures.

6. The information referred to in paragraph 5 shall include all available details, in particular the data necessary for the identification of the non-compliant AI system, the origin of the AI system, the nature of the non-compliance alleged and the risk involved, the nature and duration of the national measures taken and the arguments put forward by the relevant operator. In particular, the market surveillance authorities shall indicate whether the non-compliance is due to one or more of the following:

   (a) a failure of the AI system to meet requirements set out in Title III, Chapter 2;

   (b) shortcomings in the harmonised standards or common specifications referred to in Articles 40 and 41 conferring a presumption of conformity.

7. The market surveillance authorities of the Member States other than the market surveillance authority of the Member State initiating the procedure shall without delay inform the Commission and the other Member States of any measures adopted and of any additional information at their disposal relating to the non-compliance of the AI system concerned, and, in the event of disagreement with the notified national measure, of their objections.

8. Where, within three months of receipt of the information referred to in paragraph 5, no objection has been raised by either a Member State or the Commission in respect of a provisional measure taken by a Member State, that measure shall be deemed justified. This is without prejudice to the procedural rights of the concerned operator in accordance with Article 18 of Regulation (EU) 2019/1020.

9. The market surveillance authorities of all Member States shall ensure that appropriate restrictive measures are taken in respect of the product concerned, such as withdrawal of the product from their market, without delay.

*Article 66*
*Union safeguard procedure*

1. Where, within three months of receipt of the notification referred to in Article 65(5), objections are raised by a Member State against a measure taken by another Member State, or where the Commission considers the measure to be contrary to Union law, the Commission shall without delay enter into consultation with the relevant Member State and operator or operators and shall evaluate the national measure. On the basis of the results of that evaluation, the Commission shall decide whether the national measure is justified or not within 9 months from the notification referred to in Article 65(5) and notify such decision to the Member State concerned.

2. If the national measure is considered justified, all Member States shall take the measures necessary to ensure that the non-compliant AI system is withdrawn from their market, and shall inform the Commission accordingly. If the national measure is considered unjustified, the Member State concerned shall withdraw the measure.

3. Where the national measure is considered justified and the non-compliance of the AI system is attributed to shortcomings in the harmonised standards or common specifications referred to in Articles 40 and 41 of this Regulation, the Commission shall apply the procedure provided for in Article 11 of Regulation (EU) No 1025/2012.

*Article 67*
*Compliant AI systems which present a risk*

1. Where, having performed an evaluation under Article 65, the market surveillance authority of a Member State finds that although an AI system is in compliance with this Regulation, it presents a risk to the health or safety of persons, to the compliance with obligations under Union or national law intended to protect fundamental rights or to other aspects of public interest protection, it shall require the relevant operator to take all appropriate measures to ensure that the AI system concerned, when placed on the market or put into service, no longer presents that risk, to withdraw the AI system from the market or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe.

2. The provider or other relevant operators shall ensure that corrective action is taken in respect of all the AI systems concerned that they have made available on the market throughout the Union within the timeline prescribed by the market surveillance authority of the Member State referred to in paragraph 1.

3. The Member State shall immediately inform the Commission and the other Member States. That information shall include all available details, in particular the data necessary for the identification of the AI system concerned, the origin and the supply chain of the AI system, the nature of the risk involved and the nature and duration of the national measures taken.

4. The Commission shall without delay enter into consultation with the Member States and the relevant operator and shall evaluate the national measures taken. On the basis of the results of that evaluation, the Commission shall decide whether the measure is justified or not and, where necessary, propose appropriate measures.

5. The Commission shall address its decision to the Member States.

*Article 68*
*Formal non-compliance*

1. Where the market surveillance authority of a Member State makes one of the following findings, it shall require the relevant provider to put an end to the non-compliance concerned:

   (a) the conformity marking has been affixed in violation of Article 49;

   (b) the conformity marking has not been affixed;

   (c) the EU declaration of conformity has not been drawn up;

   (d) the EU declaration of conformity has not been drawn up correctly;

   (e) the identification number of the notified body, which is involved in the conformity assessment procedure, where applicable, has not been affixed;

2. Where the non-compliance referred to in paragraph 1 persists, the Member State concerned shall take all appropriate measures to restrict or prohibit the high-risk AI system being made available on the market or ensure that it is recalled or withdrawn from the market.

# TITLE IX

# CODES OF CONDUCT

*Article 69*
*Codes of conduct*

1. The Commission and the Member States shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application to AI systems other than high-risk AI systems of the requirements set out in Title III, Chapter 2 on the basis of technical specifications and solutions that are appropriate means of ensuring compliance with such requirements in light of the intended purpose of the systems.

2. The Commission and the Board shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application to AI systems of requirements related for example to environmental sustainability, accessibility for persons with a disability, stakeholders participation in the design and development of the AI systems and diversity of development teams on the basis of clear objectives and key performance indicators to measure the achievement of those objectives.

3. Codes of conduct may be drawn up by individual providers of AI systems or by organisations representing them or by both, including with the involvement of users and any interested stakeholders and their representative organisations. Codes of

conduct may cover one or more AI systems taking into account the similarity of the intended purpose of the relevant systems.

4. The Commission and the Board shall take into account the specific interests and needs of the small-scale providers and start-ups when encouraging and facilitating the drawing up of codes of conduct.

# TITLE X

# CONFIDENTIALITY AND PENALTIES

*Article 70*
*Confidentiality*

1. National competent authorities and notified bodies involved in the application of this Regulation shall respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular:

   (a) intellectual property rights, and confidential business information or trade secrets of a natural or legal person, including source code, except the cases referred to in Article 5 of Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure apply.

   (b) the effective implementation of this Regulation, in particular for the purpose of inspections, investigations or audits;(c) public and national security interests;

   (c) integrity of criminal or administrative proceedings.

2. Without prejudice to paragraph 1, information exchanged on a confidential basis between the national competent authorities and between national competent authorities and the Commission shall not be disclosed without the prior consultation of the originating national competent authority and the user when high-risk AI systems referred to in points 1, 6 and 7 of Annex III are used by law enforcement, immigration or asylum authorities, when such disclosure would jeopardise public and national security interests.

   When the law enforcement, immigration or asylum authorities are providers of high-risk AI systems referred to in points 1, 6 and 7 of Annex III, the technical documentation referred to in Annex IV shall remain within the premises of those authorities. Those authorities shall ensure that the market surveillance authorities referred to in Article 63(5) and (6), as applicable, can, upon request, immediately access the documentation or obtain a copy thereof. Only staff of the market surveillance authority holding the appropriate level of security clearance shall be allowed to access that documentation or any copy thereof.

3. Paragraphs 1 and 2 shall not affect the rights and obligations of the Commission, Member States and notified bodies with regard to the exchange of information and

the dissemination of warnings, nor the obligations of the parties concerned to provide information under criminal law of the Member States.

4. The Commission and Member States may exchange, where necessary, confidential information with regulatory authorities of third countries with which they have concluded bilateral or multilateral confidentiality arrangements guaranteeing an adequate level of confidentiality.

*Article 71*
*Penalties*

1. In compliance with the terms and conditions laid down in this Regulation, Member States shall lay down the rules on penalties, including administrative fines, applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are properly and effectively implemented. The penalties provided for shall be effective, proportionate, and dissuasive. They shall take into particular account the interests of small-scale providers and start-up and their economic viability.

2. The Member States shall notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

3. The following infringements shall be subject to administrative fines of up to 30 000 000 EUR or, if the offender is company, up to 6 % of its total worldwide annual turnover for the preceding financial year, whichever is higher:

   (a) non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5;

   (b) non-compliance of the AI system with the requirements laid down in Article 10.

4. The non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Articles 5 and 10, shall be subject to administrative fines of up to 20 000 000 EUR or, if the offender is a company, up to 4 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

5. The supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities in reply to a request shall be subject to administrative fines of up to 10 000 000 EUR or, if the offender is a company, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

6. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:

   (a) the nature, gravity and duration of the infringement and of its consequences;

   (b) whether administrative fines have been already applied by other market surveillance authorities to the same operator for the same infringement.

(c) the size and market share of the operator committing the infringement;

7. Each Member State shall lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fines are imposed by competent national courts of other bodies as applicable in those Member States. The application of such rules in those Member States shall have an equivalent effect.

*Article 72*
*Administrative fines on Union institutions, agencies and bodies*

1. The European Data Protection Supervisor may impose administrative fines on Union institutions, agencies and bodies falling within the scope of this Regulation. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement and of its consequences;

(b) the cooperation with the European Data Protection Supervisor in order to remedy the infringement and mitigate the possible adverse effects of the infringement, including compliance with any of the measures previously ordered by the European Data Protection Supervisor against the Union institution or agency or body concerned with regard to the same subject matter;

(c) any similar previous infringements by the Union institution, agency or body;

2. The following infringements shall be subject to administrative fines of up to 500 000 EUR:

(a) non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5;

(b) non-compliance of the AI system with the requirements laid down in Article 10.

3. The non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Articles 5 and 10, shall be subject to administrative fines of up to 250 000 EUR.

4. Before taking decisions pursuant to this Article, the European Data Protection Supervisor shall give the Union institution, agency or body which is the subject of the proceedings conducted by the European Data Protection Supervisor the opportunity of being heard on the matter regarding the possible infringement. The European Data Protection Supervisor shall base his or her decisions only on elements and circumstances on which the parties concerned have been able to comment. Complainants, if any, shall be associated closely with the proceedings.

5. The rights of defense of the parties concerned shall be fully respected in the proceedings. They shall be entitled to have access to the European Data Protection Supervisor's file, subject to the legitimate interest of individuals or undertakings in the protection of their personal data or business secrets.

6. Funds collected by imposition of fines in this Article shall be the income of the general budget of the Union.

# TITLE XI

# DELEGATION OF POWER AND COMMITTEE PROCEDURE

*Article 73*
*Exercise of the delegation*

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Article 4, Article 7(1), Article 11(3), Article 43(5) and (6) and Article 48(5) shall be conferred on the Commission for an indeterminate period of time from [*entering into force of the Regulation*].

3. The delegation of power referred to in Article 4, Article 7(1), Article 11(3), Article 43(5) and (6) and Article 48(5) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. Any delegated act adopted pursuant to Article 4, Article 7(1), Article 11(3), Article 43(5) and (6) and Article 48(5) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

*Article 74*
*Committee procedure*

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

# TITLE XII

# FINAL PROVISIONS

*Article 75*
*Amendment to Regulation (EC) No 300/2008*

In Article 4(3) of Regulation (EC) No 300/2008, the following subparagraph is added:

"When adopting detailed measures related to technical specifications and procedures for approval and use of security equipment concerning Artificial Intelligence systems in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Chapter 2, Title III of that Regulation shall be taken into account."

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …)."

*Article 76*
*Amendment to Regulation (EU) No 167/2013*

In Article 17(5) of Regulation (EU) No 167/2013, the following subparagraph is added:

"When adopting delegated acts pursuant to the first subparagraph concerning artificial intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …)."

*Article 77*
*Amendment to Regulation (EU) No 168/2013*

In Article 22(5) of Regulation (EU) No 168/2013, the following subparagraph is added:

"When adopting delegated acts pursuant to the first subparagraph concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX on [Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …)."

*Article 78*
*Amendment to Directive 2014/90/EU*

In Article 8 of Directive 2014/90/EU, the following paragraph is added:

"4. For Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, when carrying out its activities pursuant to paragraph 1 and when adopting technical specifications and testing standards in accordance with paragraphs 2 and 3, the Commission shall take into account the requirements set out in Title III, Chapter 2 of that Regulation.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).".

*Article 79*
*Amendment to Directive (EU) 2016/797*

In Article 5 of Directive (EU) 2016/797, the following paragraph is added:

"12. When adopting delegated acts pursuant to paragraph 1 and implementing acts pursuant to paragraph 11 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).".

*Article 80*
*Amendment to Regulation (EU) 2018/858*

In Article 5 of Regulation (EU) 2018/858 the following paragraph is added:

"4. When adopting delegated acts pursuant to paragraph 3 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council *, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).".

*Article 81*
*Amendment to Regulation (EU) 2018/1139*

Regulation (EU) 2018/1139 is amended as follows:

(1) In Article 17, the following paragraph is added:

"3. Without prejudice to paragraph 2, when adopting implementing acts pursuant to paragraph 1 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [*on Artificial Intelligence*] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …)."

(2) In Article 19, the following paragraph is added:

"4. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account."

(3) In Article 43, the following paragraph is added:

"4. When adopting implementing acts pursuant to paragraph 1 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account."

(4) In Article 47, the following paragraph is added:

"3. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account."

(5) In Article 57, the following paragraph is added:

"When adopting those implementing acts concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account."

(6) In Article 58, the following paragraph is added:

"3. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] , the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.".

*Article 82*
*Amendment to Regulation (EU) 2019/2144*

In Article 11 of Regulation (EU) 2019/2144, the following paragraph is added:

"3. When adopting the implementing acts pursuant to paragraph 2, concerning artificial intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

---

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).".

*Article 83*
*AI systems already placed on the market or put into service*

1. This Regulation shall not apply to the AI systems which are components of the large-scale IT systems established by the legal acts listed in Annex IX that have been placed on the market or put into service before *[12 months after the date of application of this Regulation referred to in Article 85(2)]*, unless the replacement or amendment of those legal acts leads to a significant change in the design or intended purpose of the AI system or AI systems concerned.

   The requirements laid down in this Regulation shall be taken into account, where applicable, in the evaluation of each large-scale IT systems established by the legal acts listed in Annex IX to be undertaken as provided for in those respective acts.

2. This Regulation shall apply to the high-risk AI systems, other than the ones referred to in paragraph 1, that have been placed on the market or put into service before [*date of application of this Regulation referred to in Article 85(2)*], only if, from that date, those systems are subject to significant changes in their design or intended purpose.

*Article 84*
*Evaluation and review*

1. The Commission shall assess the need for amendment of the list in Annex III once a year following the entry into force of this Regulation.

2. By [*three years after the date of application of this Regulation referred to in Article 85(2)*] and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

3. The reports referred to in paragraph 2 shall devote specific attention to the following:

   (a) the status of the financial and human resources of the national competent authorities in order to effectively perform the tasks assigned to them under this Regulation;

   (b) the state of penalties, and notably administrative fines as referred to in Article 71(1), applied by Member States to infringements of the provisions of this Regulation.

4. Within [*three years after the date of application of this Regulation referred to in Article 85(2)*] and every four years thereafter, the Commission shall evaluate the impact and effectiveness of codes of conduct to foster the application of the requirements set out in Title III, Chapter 2 and possibly other additional requirements for AI systems other than high-risk AI systems.

5. For the purpose of paragraphs 1 to 4 the Board, the Member States and national competent authorities shall provide the Commission with information on its request.

6. In carrying out the evaluations and reviews referred to in paragraphs 1 to 4 the Commission shall take into account the positions and findings of the Board, of the European Parliament, of the Council, and of other relevant bodies or sources.

7. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account developments in technology and in the light of the state of progress in the information society.

*Article 85*
*Entry into force and application*

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. This Regulation shall apply from [24 months following the entering into force of the Regulation].

3. By way of derogation from paragraph 2:

   (a) Title III, Chapter 4 and Title VI shall apply from [three months following the entry into force of this Regulation];

   (b) Article 71 shall apply from [twelve months following the entry into force of this Regulation].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

| | |
|---|---|
| *For the European Parliament* | *For the Council* |
| *The President* | *The President* |

# LEGISLATIVE FINANCIAL STATEMENT

## 1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

1.2. Policy area(s) concerned

1.3. The proposal/initiative relates to:

1.4. Objective(s)

1.4.1. General objective(s)

1.4.2. Specific objective(s)

1.4.3. Expected result(s) and impact

1.4.4. Indicators of performance

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone

1.5.3. Lessons learned from similar experiences in the past

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

1.5.5 Assessment of the different available financing options, including scope for redeployment

1.6. Duration and financial impact of the proposal/initiative

1.7. Management mode(s) planned

## 2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

2.2. Management and control system

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

2.3. Measures to prevent fraud and irregularities

## 3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

3.2. Estimated financial impact of the proposal on appropriations

*3.2.1. Summary of estimated impact on operational appropriations*

*3.2.2. Estimated output funded with operational appropriations*

*3.2.3. Summary of estimated impact on administrative appropriations*

*3.2.4. Compatibility with the current multiannual financial framework*

*3.2.5. Third-party contributions*

3.3. Estimated impact on revenue

# LEGISLATIVE FINANCIAL STATEMENT

## 1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

### 1.1. Title of the proposal/initiative

| |
|---|
| Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts |

### 1.2. Policy area(s) concerned

| |
|---|
| Communications Networks, Content and Technology;<br><br>Internal Market, Industry, Entrepreneurship and SMEs;<br><br>The budgetary impact concerns the new tasks entrusted with the Commission, including the support to the EU AI Board;<br><br>Activity: Shaping Europe's digital future. |

### 1.3. The proposal/initiative relates to:

X **a new action**

☐ **a new action following a pilot project/preparatory action**[64]

☐ **the extension of an existing action**

☐ **an action redirected towards a new action**

### 1.4. Objective(s)

*1.4.1. General objective(s)*

| |
|---|
| The general objective of the intervention is to ensure the proper functioning of the single market by creating the conditions for the development and use of trustworthy artificial intelligence in the Union. |

*1.4.2. Specific objective(s)*

| |
|---|
| Specific objective No 1<br><br>To set requirements specific to AI systems and obligations on all value chain participants in order to ensure that AI systems placed on the market and used are safe and respect existing law on fundamental rights and Union values;<br><br>Specific objective No 2 |

64 As referred to in Article 54(2)(a) or (b) of the Financial Regulation

To ensure legal certainty to facilitate investment and innovation in AI by making it clear what essential requirements, obligations, as well as conformity and compliance procedures must be followed to place or use an AI system in the Union market;

Specific objective No 3

To enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems by providing new powers, resources and clear rules for relevant authorities on conformity assessment and ex post monitoring procedures and the division of governance and supervision tasks between national and EU levels;

Specific objective No 4

To facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation by taking EU action to set minimum requirement for AI systems to be placed and used in the Union market in compliance with existing law on fundamental rights and safety.

*1.4.3. Expected result(s) and impact*

*Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.*

AI suppliers should benefit from a minimal but clear set of requirements, creating legal certainty and ensuring access to the entire single market.

AI users should benefit from legal certainty that the high-risk AI systems they buy comply with European laws and values.

Consumers should benefit by reducing the risk of violations of their safety or fundamental rights.

*1.4.4. Indicators of performance*

*Specify the indicators for monitoring implementation of the proposal/initiative.*

Indicator 1

Number of serious incidents or AI performances which constitute a serious incident or a breach of fundamental rights obligations (semi-annual) by fields of applications and calculated a) in absolute terms, b) as share of applications deployed and c) as share of citizens concerned.

Indicator 2

a) Total AI investment in the EU (annual)

b) Total AI investment by Member State (annual)

c) Share of companies using AI (annual)

d) Share of SMEs using AI (annual)

a) and b) will be calculated based on official sources and benchmarked against private estimates

c) and d) will be collected by regular company surveys

**1.5. Grounds for the proposal/initiative**

*1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative*

The Regulation should be fully applicable one year and a half after its adoption. However, elements of the governance structure should be in place before then. In particular, Member States shall have appointed existing authorities and/or established new authorities performing the tasks set out in the legislation earlier, and the EU AI Board should be set-up and effective. By the time of applicability, the European database of AI systems should be fully operative. In parallel to the adoption process, it is therefore necessary to develop the database, so that its development has come to an end when the regulation enters into force.

*1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.*

An emerging patchy framework of potentially divergent national rules will hamper the seamless provision of AI systems across the EU and is ineffective in ensuring the safety and protection of fundamental rights and Union values across the different Member States. A common EU legislative action on AI could boost the internal market and has great potential to provide European industry with a competitive edge at the global scene and economies of scale that cannot be achieved by individual Member States alone.

*1.5.3. Lessons learned from similar experiences in the past*

The E-commerce Directive 2000/31/EC provides the core framework for the functioning of the single market and the supervision of digital services and sets a basic structure for a general cooperation mechanism among Member States, covering in principle all requirements applicable to digital services. The evaluation of the Directive pointed to shortcomings in several aspects of this cooperation mechanism, including important procedural aspects such as the lack of clear timeframes for response from Member States coupled with a general lack of responsiveness to requests from their counterparts. This has led over the years to a lack of trust between Member States in addressing concerns about providers offering digital services cross-border. The evaluation of the Directive showed the need to define a differentiated set of rules and requirements at European level. For this reason, the implementation of the specific obligations laid down in this Regulation would require a specific cooperation mechanism at EU level, with a governance structure ensuring coordination of specific responsible bodies at EU level.

*1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments*

The Regulation Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts defines a new common framework of requirements applicable to AI systems, which goes well beyond the framework provided by existing legislation. For this reason, a new national and European regulatory and coordination function needs to be established with this proposal.

As regards possible synergies with other appropriate instruments, the role of notifying authorities at national level can be performed by national authorities fulfilling similar functions sunder other EU regulations.

Moreover, by increasing trust in AI and thus encouraging investment in development and adoption of AI, it complements Digital Europe, for which promoting the diffusion of AI is one of five priorities.

*1.5.5. Assessment of the different available financing options, including scope for redeployment*

| |
|---|
| The staff will be redeployed. The other costs will be supported from the DEP. envelope, given that the objective of this regulation – ensuring trustworthy AI – contributes directly to one key objective of Digital Europe – accelerating AI development and deployment in Europe. |

## 1.6. Duration and financial impact of the proposal/initiative

☐ **limited duration**

– ☐ in effect from [DD/MM]YYYY to [DD/MM]YYYY

– ☐ Financial impact from YYYY to YYYY for commitment appropriations and from YYYY to YYYY for payment appropriations.

X **unlimited duration**

– Implementation with a start-up period from one/two (tbc) year,

– followed by full-scale operation.

## 1.7. Management mode(s) planned[65]

X **Direct management** by the Commission

– ☐ by its departments, including by its staff in the Union delegations;

– ☐ by the executive agencies

☐ **Shared management** with the Member States

☐ **Indirect management** by entrusting budget implementation tasks to:

– ☐ third countries or the bodies they have designated;

– ☐ international organisations and their agencies (to be specified);

– ☐ the EIB and the European Investment Fund;

– ☐ bodies referred to in Articles 70 and 71 of the Financial Regulation;

– ☐ public law bodies;

– ☐ bodies governed by private law with a public service mission to the extent that they provide adequate financial guarantees;

– ☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that provide adequate financial guarantees;

– ☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

– *If more than one management mode is indicated, please provide details in the 'Comments' section.*

Comments

---

[65] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

## 2. MANAGEMENT MEASURES

### 2.1. Monitoring and reporting rules

*Specify frequency and conditions.*

| |
|---|
| The Regulation will be reviewed and evaluated five years from the entry into force of the regulation. The Commission will report on the findings of the evaluation to the European Parliament, the Council and the European Economic and Social Committee. |

### 2.2. Management and control system(s)

*2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed*

| |
|---|
| The Regulation establishes a new policy with regard to harmonised rules for the provision of artificial intelligence systems in the internal market while ensuring the respect of safety and fundamental rights. These new rules require a consistency mechanism for the cross-border application of the obligations under this Regulation in the form of a new advisory group coordinating the activities of national authorities.<br><br>In order to face these new tasks, it is necessary to appropriately resource the Commission's services. The enforcement of the new Regulation is estimated to require 10 FTE à regime (5 FTE for the support to the activities of the Board and 5 FTE for the European Data Protection Supervisor acting as a notifying body for AI systems deployed by a body of the European Union). |

*2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them*

| |
|---|
| In order to ensure that the members of the Board have the possibility to make informed analysis on the basis of factual evidence, it is foreseen that the Board should be supported by the administrative structure of the Commission and that an expert group be created to provide additional expertise where required. |

*2.2.3. Estimate and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)*

| |
|---|
| For the meeting expenditure, given the low value per transaction (e.g. refunding travel costs for a delegate for a meeting), standard control procedures seem sufficient. Regarding the development of the database, contract attribution has a strong internal control system in place in DG CNECT through centralised procurement activities. |

### 2.3. Measures to prevent fraud and irregularities

*Specify existing or envisaged prevention and protection measures, e.g. from the Anti-Fraud Strategy.*

The existing fraud prevention measures applicable to the Commission will cover the additional appropriations necessary for this Regulation.

## 3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

### 3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

| Heading of multiannual financial framework | Budget line | Type of expenditure | Contribution | | | |
|---|---|---|---|---|---|---|
| | Number | Diff./Non-diff.[66] | from EFTA countries [67] | from candidate countries[68] | from third countries | within the meaning of Article 21(2)(b) of the Financial Regulation |
| 7 | 20 02 06 Administrative expenditure | Non-diff. | NO | NO | NO | NO |
| 1 | 02 04 03 DEP Artificial Intelligence | Diff. | YES | NO | NO | NO |
| 1 | 02 01 30 01 Support expenditure for the Digital Europe programme | Non-diff. | YES | NO | NO | NO |

### 3.2. Estimated financial impact of the proposal on appropriations

*3.2.1. Summary of estimated impact on expenditure on operational appropriations*

– ☐ The proposal/initiative does not require the use of operational appropriations

66 Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.
67 EFTA: European Free Trade Association.
68 Candidate countries and, where applicable, potential candidate countries from the Western Balkans.

– X The proposal/initiative requires the use of operational appropriations, as explained below:

EUR million (to three decimal places)

| **Heading of multiannual financial framework** | 1 | |
|---|---|---|

| DG: CNECT | | | | Year **2022** | Year **2023** | Year **2024** | Year **2025** | Year **2026** | Year **2027**[69] | **TOTAL** | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| • Operational appropriations | | | | | | | | | | | |
| Budget line[70] 02 04 03 | | Commitments | (1a) | | 1.000 | | | | | | **1.000** |
| | | Payments | (2a) | | 0.600 | 0.100 | 0.100 | 0.100 | 0.100 | | **1.000** |
| Budget line | | Commitments | (1b) | | | | | | | | |
| | | Payments | (2b) | | | | | | | | |
| Appropriations of an administrative nature financed from the envelope of specific programmes[71] | | | | | | | | | | | |
| Budget line 02 01 30 01 | | | (3) | | 0.240 | 0.240 | 0.240 | 0.240 | 0.240 | | **1.200** |
| **TOTAL appropriations for DG CNECT** | | Commitments | =1a+1b +3 | | **1.240** | | **0.240** | **0.240** | **0.240** | | **2.200** |
| | | Payments | =2a+2b +3 | | **0.840** | **0.340** | **0.340** | **0.340** | **0.340** | | **2.200** |

69 Indicative and dependent on budget availability.
70 According to the official budget nomenclature.
71 Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| • TOTAL operational appropriations | Commitments | (4) | | 1.000 | | | | | | **1.000** |
| | Payments | (5) | | 0.600 | 0.100 | 0.100 | 0.100 | 0.100 | | **1.000** |
| • TOTAL appropriations of an administrative nature financed from the envelope for specific programmes | | (6) | | **0.240** | **0.240** | **0.240** | **0.240** | **0.240** | | **1.200** |
| **TOTAL appropriations under HEADING 1** of the multiannual financial framework | Commitments | =4+ 6 | | 1.240 | 0.240 | 0.240 | .0.240 | 0.240 | | **2.200** |
| | Payments | =5+ 6 | | 0.840 | 0.340 | 0.340 | 0.340 | 0.340 | | **2.200** |

**If more than one heading is affected by the proposal / initiative, repeat the section above:**

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| • TOTAL operational appropriations (all operational headings) | Commitments | (4) | | | | | | | | |
| | Payments | (5) | | | | | | | | |
| • TOTAL appropriations of an administrative nature financed from the envelope for specific programmes (all operational headings) | | (6) | | | | | | | | |
| **TOTAL appropriations under HEADINGS 1 to 6** of the multiannual financial framework (Reference amount) | Commitments | =4+ 6 | | | | | | | | |
| | Payments | =5+ 6 | | | | | | | | |

| Heading of multiannual financial framework | 7 | 'Administrative expenditure' |
|---|---|---|

This section should be filled in using the 'budget data of an administrative nature' to be firstly introduced in the Annex to the Legislative Financial Statement (Annex V to the internal rules), which is uploaded to DECIDE for interservice consultation purposes.

EUR million (to three decimal places)

| | | Year **2023** | Year **2024** | Year **2025** | Year **2026** | Year **2027** | **After 2027**[72] | **TOTAL** |
|---|---|---|---|---|---|---|---|---|
| DG: CNECT | | | | | | | | |
| • Human resources | | 0.760 | 0.760 | 0.760 | 0.760 | 0.760 | 0.760 | **3.800** |
| • Other administrative expenditure | | **0.010** | **0.010** | **0.010** | **0.010** | **0.010** | **0.010** | **0.050** |
| **TOTAL DG CNECT** | **Appropriations** | **0.760** | **0.760** | **0.760** | **0.760** | **0.760** | **0.760** | **3.850** |
| European Data Protection Supervisor | | | | | | | | |
| • Human resources | | 0.760 | 0.760 | 0.760 | 0.760 | 0.760 | 0.760 | **3.800** |
| • Other administrative expenditure | | | | | | | | |
| **TOTAL EDPS** | **Appropriations** | **0.760** | **0.760** | **0.760** | **0.760** | **0.760** | **0.760** | **3.800** |
| **TOTAL appropriations under HEADING 7** of the multiannual financial framework | (Total commitments = Total payments) | 1.530 | 1.530 | 1.530 | 1.530 | 1.530 | 1.530 | **7.650** |

EUR million (to three decimal places)

| | Year | Year | Year | Year | Year **2026** | Year **2027** | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|

[72] All figures in this column are indicative and subject to the continuation of the programmes and availability of appropriations

| | | 2022 | 2023 | 2024 | 2025 | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **TOTAL appropriations under HEADINGS 1 to 7** of the multiannual financial framework | Commitments | | 2.770 | 1.770 | 1.770 | 1.770 | 1.770 | | **9.850** |
| | Payments | | 2.370 | 1.870 | 1.870 | 1.870 | 1.870 | | **9.850** |

*3.2.2. Estimated output funded with operational appropriations*

Commitment appropriations in EUR million (to three decimal places)

| **Indicate objectives and outputs** ⇩ | | | Year **2022** | | Year **2023** | | Year **2024** | | Year **2025** | | Year **2026** | | Year **2027** | | After **2027**[73] | | **TOTAL** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **OUTPUTS** | | | | | | | | | | | | | | | | | |
| | Type | Average cost | No | Cost | No | Cost | No | Cost | No | Cost | No | Cost | No | Cost | No | Cost | Tota l No | Total cost |
| SPECIFIC OBJECTIVE No 1[74]… | | | | | | | | | | | | | | | | | | |
| Database | | | | | 1 | 1.000 | 1 | | 1 | | 1 | | 1 | | 1 | 0.100 | 1 | 1.000 |
| Meetings- Output | | | | | 10 | 0.200 | 10 | 0.200 | 10 | 0.200 | 10 | 0.200 | 10 | 0.200 | 10 | 0.200 | 50 | 1.000 |
| Communication activities | | | | | 2 | 0.040 | 2 | 0.040 | 2 | 0.040 | 2 | 0.040 | 2 | 0.040 | 2 | 0.040 | 10 | 0.040 |
| Subtotal for specific objective No 1 | | | | | | | | | | | | | | | | | | |
| SPECIFIC OBJECTIVE No 2 ... | | | | | | | | | | | | | | | | | | |
| - Output | | | | | | | | | | | | | | | | | | |
| Subtotal for specific objective No 2 | | | | | | | | | | | | | | | | | | |

[73] All figures in this column are indicative and subject to the continuation of the programmes and availability of appropriations

[74] As described in point 1.4.2. 'Specific objective(s)…'

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **TOTALS** | | | 13 | 0.240 | 13 | 0.240 | 13 | 0.240 | 13 | 0.240 | 13 | 0.240 | 13 | 0.100 | 65 | 2.200 |

### *3.2.3. Summary of estimated impact on administrative appropriations*

– ☐ The proposal/initiative does not require the use of appropriations of an administrative nature

– X The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

| | Year **2022** | Year **2023** | Year **2024** | Year **2025** | Year **2026** | Year **2027** | **Yearly after 2027**[75] | **TOTAL** |
|---|---|---|---|---|---|---|---|---|
| **HEADING 7 of the multiannual financial framework** | | | | | | | | |
| Human resources | | 1.520 | 1.520 | 1.520 | 1.520 | 1.520 | **1.520** | **7.600** |
| Other administrative expenditure | | 0.010 | 0.010 | 0.010 | 0.010 | 0.010 | **0.010** | **0.050** |
| **Subtotal HEADING 7 of the multiannual financial framework** | | 1.530 | 1.530 | 1.530 | 1.530 | 1.530 | **1.530** | **7.650** |
| **Outside HEADING 7**[76] **of the multiannual financial framework** | | | | | | | | |
| Human resources | | | | | | | | |
| Other expenditure of an administrative nature | | 0.240 | 0.240 | 0.240 | 0.240 | 0.240 | **0.240** | **1.20** |
| **Subtotal outside HEADING 7 of the multiannual financial framework** | | 0.240 | 0.240 | 0.240 | 0.240 | 0.240 | **0.240** | **1.20** |
| **TOTAL** | | **1.770** | **1.770** | **1.770** | **1.770** | **1.770** | **1.770** | **8.850** |

The appropriations required for human resources and other expenditure of an administrative nature will be met by appropriations from the DG that are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

75 All figures in this column are indicative and subject to the continuation of the programmes and availability of appropriations.

76 Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

3.2.3.1. Estimated requirements of human resources

– ☐ The proposal/initiative does not require the use of human resources.

– X The proposal/initiative requires the use of human resources, as explained below:

*Estimate to be expressed in full time equivalent units*

| . | | Year **2023** | Year **2024** | Year **2025** | **2026** | **2027** | **After 2027**[77] | |
|---|---|---|---|---|---|---|---|---|
| **• Establishment plan posts (officials and temporary staff)** | | | | | | | | |
| 20 01 02 01 (Headquarters and Commission's Representation Offices) | | 10 | 10 | 10 | 10 | 10 | 10 | |
| 20 01 02 03 (Delegations) | | | | | | | | |
| 01 01 01 01 (Indirect research) | | | | | | | | |
| 01 01 01 11 (Direct research) | | | | | | | | |
| Other budget lines (specify) | | | | | | | | |
| **• External staff (in Full Time Equivalent unit: FTE)**[78] | | | | | | | | |
| 20 02 01 (AC, END, INT from the 'global envelope') | | | | | | | | |
| 20 02 03 (AC, AL, END, INT and JPD in the delegations) | | | | | | | | |
| **XX** 01 xx **yy zz** [79] | - at Headquarters | | | | | | | |
| | - in Delegations | | | | | | | |
| 01 01 01 02 (AC, END, INT - Indirect research) | | | | | | | | |
| 01 01 01 12 (AC, END, INT - Direct research) | | | | | | | | |
| Other budget lines (specify) | | | | | | | | |
| **TOTAL** | | **10** | **10** | **10** | **10** | **10** | **10** | |

**XX** is the policy area or budget title concerned.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

EDPS is expected to provide half of the resources required.

Description of tasks to be carried out:

| | |
|---|---|
| Officials and temporary staff | To prepare a total of 13-16 meetings, draft reports, continue policy work, e.g. regarding future amendments of the list of high-risk AI applications, and maintain relations with Member States' authorities will require four AD FTE and 1 AST FTE. |

[77] All figures in this column are indicative and subject to the continuation of the programmes and availability of appropriations.

[78] AC = Contract Staff; AL = Local Staff; END = Seconded National Expert; INT = agency staff; JPD = Junior Professionals in Delegations.

[79] Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

| | |
|---|---|
| | For AI systems developed by the EU institutions, the European Data Protection Supervisor is responsible. Based on past experience, it can be estimated that 5 AD FTE are reuqired to fulfill the EDPS responsibilites under the draft legislation. |
| External staff | |

*3.2.4. Compatibility with the current multiannual financial framework*

The proposal/initiative:

– X can be fully financed through redeployment within the relevant heading of the Multiannual Financial Framework (MFF).

| No reporgramming is needed. |
|---|

– ☐ requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation.

| Explain what is required, specifying the headings and budget lines concerned, the corresponding amounts, and the instruments proposed to be used. |
|---|

– ☐ requires a revision of the MFF.

| Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts. |
|---|

*3.2.5. Third-party contributions*

The proposal/initiative:

– X does not provide for co-financing by third parties

– ☐ provides for the co-financing by third parties estimated below:

Appropriations in EUR million (to three decimal places)

| | Year **N**[80] | Year **N+1** | Year **N+2** | Year **N+3** | Enter as many years as necessary to show the duration of the impact (see point 1.6) | | | Total |
|---|---|---|---|---|---|---|---|---|
| Specify the co-financing body | | | | | | | | |
| TOTAL appropriations co-financed | | | | | | | | |

[80] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

### 3.3. Estimated impact on revenue

– ☐ The proposal/initiative has the following financial impact:

– ☐ The proposal/initiative has the following financial impact:

– ☐ on other revenue

– ☐ on other revenue

– Please indicate, if the revenue is assigned to expenditure lines ☐

EUR million (to three decimal places)

| Budget revenue line: | Appropriations available for the current financial year | Impact of the proposal/initiative[81] | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Year **N** | Year **N+1** | Year **N+2** | Year **N+3** | Enter as many years as necessary to show the duration of the impact (see point 1.6) | | |
| Article ……. | | | | | | | | |

For assigned revenue, specify the budget expenditure line(s) affected.

Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

[81] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.